Lauri Nurmi

StoneGate-palomuurin virtualisointi

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikka
Insinöörityö
24.3.2012

Metropolia

Tiivistelmä

Tekijä Otsikko Sivumäärä Aika	Lauri Nurmi StoneGate-palomuurin virtualisointi 65 sivua 24.3.2012
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja	yliopettaja Markku Nuutinen

Opinnäytetyön pääasiallisena tavoitteena oli tutustua StoneGate-palomuuriratkaisuun ja sen virtualisointiin. Virtualisoinnin kehitys ja kasvu on tuonut esiin uusia haasteita tietoturvan saralla. Työssä kävi ilmi, että virtuaalisten ympäristöjen tietoturva on laajalti huonosti huomioitu. Työssä selvitettiin, millaisia ratkaisuja virtuaalisen tietoturvan haasteisiin on tarjolla. Yhden niistä eli Stonesoft Oyj:n StoneGate-palomuurin virtuaalisen version toimintaa tutkittiin ja testattiin sitä varten rakennetussa testiympäristössä.

Virtualisointialustat jaoteltiin työssä kahteen eri tyyppiin eli hosted- ja hypervisor-arkkitehtuureihin. Virtualisointialustoista käytiin läpi VMwaren ESX, ESXi ja Workstation, joista jälkimmäistä käytettiin testauksessa. Virtuaalisten tietoturvaratkaisujen vertailussa esiin tulivat VMwaren VMsafe-rajapinta ja perinteiset virtuaalikoneissa ajettavat tietoturvalaitteet, kuten StoneGate. VMsafen avulla tietoturvalaitteen voi integroida hypervisoriin, joka tarjoaa laitteelle kokonaisvaltaisen näkymän muun muassa virtuaalisen verkon liikenteeseen.

Suorituskyvyn ja hallinnan kannalta ylivoimainen VMsafe tulee olemaan tärkeässä asemassa virtuaalisen tietoturvan kehityksessä vaikka sitä hyödyntäviä tuotteita on vielä hyvin vähän. Testauksen perusteella StoneGate-palomuurien suorituskyky ja hallittavuus todettiin hyväksi ja tuotteesta saatiin hyviä käytännön kokemuksia. Oikeat tuotantotestit tuotteella vaatisivat silti paljon laajempaa ja pidempiaikaista testausta.

Avainsanat	StoneGate, VMware, VMsafe, virtualisointi, palomuuri

Metropolia

Abstract

Author Title Number of Pages Date	Lauri Nurmi Virtualizing a StoneGate firewall 65 pages 24 March 2012
Degree	Bachelor of Engineering
Degree Programme	Degree Programme in Information Technology
Specialisation option	Telecommunications and Data Networks
Instructor	Markku Nuutinen, Principal Lecturer

The main goal of this thesis was to get acquainted with the StoneGate virtual firewall solution. The rise of virtualization has brought forth new challenges in information security. It was found that at large, the state of information security in virtual environments is poor. One goal was to determine what kinds of solutions exist to battle the poor state of virtual security. One such solution, the StoneGate virtual firewall made by Stonesoft Corporation, was examined and tested in a virtual environment.

Virtualization products were divided into two categories: products based on either hosted or hypervisor architectures. VMware products ESX, ESXi and Workstation were examined in more detail and the latter was used in the testing. Comparing virtual security solutions, two varieties came to the fore, VMware's VMsafe and traditional solutions such as StoneGate which are ran in virtual machines. With VMsafe a security solution can be integrated into the hypervisor which offers a more comprehensive view of all virtual network traffic.

VMsafe and other hypervisor based security products were found in theory to have superior performance and manageability compared to the traditional solutions. The downside is that there are still very few products that take advantage of VMsafe. The testing proved the performance and manageability of the StoneGate firewalls also to be very good. Actual production tests with the product would still have to be more thorough and extensive.

Keywords	StoneGate, VMware, VMsafe, virtualization, firewall

Sisällys

1 Johdanto 1

2 Verkkoprotokollat 1

2.1 TCP/IP-viitemalli 1
2.1.1 TCP-protokolla 4
2.1.2 UDP-protokolla 5
2.1.3 IPv4-protokolla 6
2.1.4 IPv6-protokolla 9
2.2 OSI-malli 10

3 Palomuurit 11

3.1 Palomuurien ominaisuuksia ja historiaa 12
3.2 StoneGate-palomuuriratkaisu 18

4 Virtualisointi 23

4.1 Virtualisoinnin perusteita 23
4.2 VMware-virtualisointiratkaisut 27
4.3 Virtuaaliset tietoverkot 29
4.4 Virtuaaliympäristön tietoturva 33

5 Virtuaalinen testiympäristö 38

5.1 Topologia ja suunnitteluperiaatteet 38
5.2 Vmware Workstationin asennus 42
5.3 StoneGate Management Centerin asennus 46
5.4 Palomuurien käyttöönotto SMC:n kanssa 49
5.5 Klusterin vikasietoisuuden testaus 56
5.6 Käyttötapaus klusterin päivitys 59

6 Yhteenveto 60

Lähteet 62

1 Johdanto

Virtualisointi on tietotekniikassa kasvava trendi, jonka tietoturvaan tulisi suhtautua huolella. Opinnäytetyön tavoitteena on tutustua ensin tarkemmin tietoverkkojen ja palomuurien teoriaan ja kehitykseen. Tämän jälkeen tutustutaan virtualisointiin ja VMwaren tuotteisiin, tietoturvaan virtuaaliympäristössä ja lopulta fyysisiin ja virtuaalisiin StoneGate-palomuureihin. Pääasiallinen tavoite on selvittää miten StoneGate-palomuuriratkaisut ja niiden virtualisointi toimii käytännössä. Tavoitteena on myös verrata erilaisia olemassaolevia virtuaalisia tietoturvaratkaisuja. Työssä tehtäviä käytännön testejä varten rakennettiin virtuaalinen testiympäristö, joka oli riittävän monipuolinen virtuaalisten palomuurien toiminnan ja käyttöönoton edellytysten ja haasteiden määrittämiseksi.

2 Verkkoprotokollat

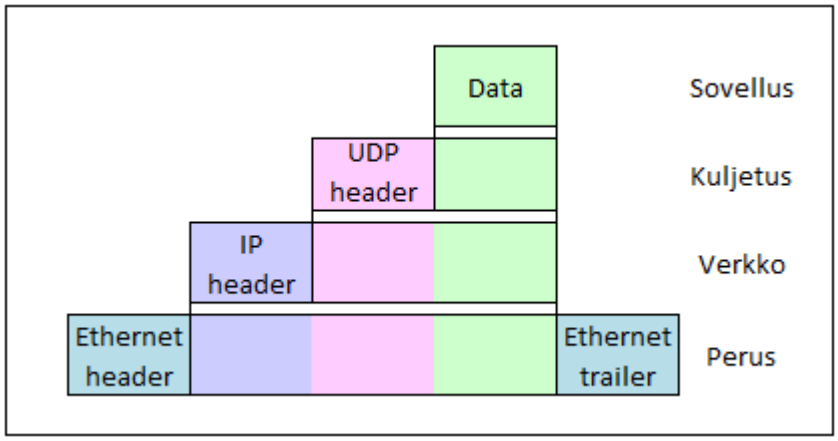
2.1 TCP/IP-viitemalli

TCP/IP-viitemalli on nykyään yleisin käytössä oleva tietoverkkojen viitemalli. Malli on nimetty sen kahden pääprotokollan, TCP:n ja IP:n mukaan. TCP/IP sisältää suuren kokoelman protokollia, jotka on jaettu eri kerroksiin tietokoneiden väliseen kommunikointiin. TCP/IP koostuu neljästä kerroksesta, joiden protokollat vastaavat tietyistä osista tietokoneiden välisessä kommunikaatiossa. Taulukossa 1 kuvatut kerrokset ovat viitemallissa niin sanotusti ylhäältä alas: sovelluskerros eli application layer, kuljetuskerros eli transport layer, verkkokerros eli internet layer ja peruskerros eli link layer tai network access layer. Mitä alemmas viitemallissa mennään, sitä erikoistuneempaa osaa kommunikaatiossa sen kerroksen protokollat hoitavat: sovelluskerros on vuorovaikutuksessa sovellusten kanssa, kuljetuskerros huolehtii tiedonvälityksestä, verkkokerros siitä, miten paketit pääsevät perille ja peruskerros siitä, miten bitit välitetään valitussa fyysisessä mediassa. Viitemallin mukaisesti jokainen kerros tarjoaakin palveluita sitä ylemmälle kerrokselle. (1, s. 22.)

Taulukko 1. TCP/IP-viitemallin kerrokset ja esimerkkiprotokollia.

TCP/IP kerros	Esimerkkiprotokollia
Sovellus	HTTP, SMTP, FTP, SSH
Kuljetus	TCP, UDP
Verkko	IP, ICMP
Perus	Ethernet, PPP, Frame Relay

Viitemalliin kuuluu olennaisena osana enkapsuloinnin käsite, jota kuvio 1 havainnollistaa. Jokainen kerros, usein sovelluskerros poislukien, lisää omat otsakkeensa (engl. header) ja joissain tapauksissa myös lopukkeensa (engl. trailer) ylemmältä kerrokselta saamansa datan ympärille. Enkapsuloinnin takia mikään kerros ei periaatteessa ole tietoinen ylemmän tason protokollista ja yhteyksistä. Enkapsuloitua kokonaisuutta kutsutaan terminologian selvyyden vuoksi kuljetuskerroksella segmentiksi, verkkokerroksella paketiksi ja peruskerroksella kehykseksi. (1, s. 30—31.)



Kuvio 1. Esimerkki sovellusdatan enkapsuloinnista UDP:stä Ethernet-kehykseksi.

Sovelluskerroksen protokollat tarjoavat palveluita tietokoneella ajettaville ohjelmille, esimerkiksi mahdollisuuden siirtää tiedostoja selaimella HTTP:n välityksellä. Sovelluskerroksella on ymmärrettävästi melko suuri määrä protokollia erilaisten sovellusten lukumäärän takia. (1, s. 23—25.)

Kuljetuskerros mahdollistaa tiedonvälityksen tietokoneiden välillä, protokollasta riippuen myös luotettavasti. Kerroksen protokollat myös segmentoivat datan enkapsulointia varten ja mahdollistavat yhteyksien multipleksoinnin käyttämällä porttinumeroita. Kaksi yleisimmin kuljetuskerroksella käytettyä protokollaa ovat TCP

(Transmission Control Protocol) ja UDP (User Datagram Protocol), joista TCP tarjoaa laajan valikoiman palveluita sovelluksille, kun taas UDP ei. Lähde- ja kohdelaitteiden valitsema kuljetuskerroksen protokolla segmentoi datan lähetykseen sopiviin osiin, TCP-yhteydessä koneet sopivat segmenttikoon yhteyden muodostuksen aikana kun taas UDP segmentoi datan pelkästään lähdelaitteen suurimman salliman pakettikoon mukaan. Suurin pakettikoko eli Maximum Transmission Unit (MTU) on mediatyyppikohtainen arvo, jonka määritys on peruskerroksen tehtävä. Se voidaan myös määritellä manuaalisesti, jonkin protokollan avulla tai automaattisesti käyttöjärjestelmään mediatyypille asetetun oletusarvon mukaan. (1, s. 133; 2.)

Verkkokerros pitää huolta vain pakettien kuljetuksesta kohteeseensa, tosin se ei takaa pakettien perillepääsyä. Internet Protol eli IP-protokolla on pitkälti ainut nykyään käytössä oleva verkkokerroksen protokolla monipuolisuutensa ansiosta, IP on suunniteltu sillä periaatteella, että sitä voidaan ajaa miltei missä tahansa verkossa ja miltei mitä tahansa sovellusta voidaan ajaa IP:tä käyttäen. Yksi verkon toiminnan kannalta tärkeä toinen verkkokerroksen protokolla on ICMP eli Internet Control Message Protocol, joka perustuu IP-protokollaan. Nimensä mukaisesti tällä kontrolliprotokollalla voidaan viestittää lähettäjälle esimerkiksi, että pakettia ei voitu toimittaa, koska kohdelaite ei vastaa tai kohdeverkko on saavuttamattomissa. Reitittimet, jotka yhdistävät eri verkon osia, ovat vastuussa IP-pakettien toimituksesta oikeaan määränpäähänsä. Verkkokerros ei ole tietoinen ylempien kerrosten yhteyksistä vaan jokainen IP-paketti käsitellään yksitellen, jolloin kaksi peräkkäistäkin pakettia voi päästä kohteeseensa eri reittejä. IP-paketit reititetään kohteisiinsa loogisten osoitteiden avulla, joita kutsutaan IP-osoitteiksi, julkiset internetiin julkaistut osoitteet ovat uniikkeja, jolloin jokaisella paketilla on yksiselitteinen vastaanottaja. Julkisten IP-osoitteiden jakelua hoitavat omat järjestönsä, jotka varmistavat, ettei samaa osoitetta jaeta useammalla taholle. (1, s. 27.)

Peruskerros määrittää, kuinka laite liitetään fyysiseen mediaan ja miten dataa siirretään kyseisessä mediassa linkin toiseen päähän. TCP/IP on suunniteltu laitteistoriippumattomaksi, eli peruskerroksen protokollat hoitavat tiedonsiirron missä tahansa mediassa ja ylempien kerrosten ei tarvitse tietää verkon konkreettisesta toteutuksesta mitään. Kerros täten käsittääkin melko suuren määrän protokollia lähiverkkoyhteyksistä, kuten Ethernet ja WLAN, laajaverkkoyhteyksiin, kuten Frame

Relay ja Point-to-Point Protocol eli PPP. Jotta kerros pystyy lähettämään kehyksiä sen pitää pystyä yhdistämään loogiset IP-osoitteet fyysisiin MAC eli Media Access Control -osoitteisiin. Tämä toteutetaan Address Resolution Protocol:in eli ARP:n avulla, laitteet lähettävät ja vastaavat ARP-kyselyihin joiden perusteella ne pystyvät yhdistämään IP:t MAC-osoitteisiin. Toiminnallisuus on tarpeen vain niin sanotuissa multiaccess-verkoissa kuten Ethernetissä, jossa yhteen verkkosegmenttiin on yhdistetty useampi laite. (1, s. 28—30; 3.)

2.1.1 TCP-protokolla

TCP tarjoaa useita palveluita suuremman siirtokaistan käytön ja prosessoriajan kustannuksella. Mainitun multipleksoinnin lisäksi se tarjoaa vuonhallintaa, virheenkorjausta ja yhteydenhallintaa, jotka toteutetaan kuviossa 2 esitettyjen otsakkeen kenttien avulla. Vuonhallinta on toteutettu ikkunan koko -kentän avulla, ikkuna tarkoittaa, kuinka monta kuittaamatonta tavua voidaan lähettää ennen kuin niitä pitää kuitata. Ikkunan koko on dynaaminen arvo, jota kasvatetaan niin kauan, kunnes alkaa ilmetä virheitä, eli kaikki paketit eivät enää tule perille. Tämän ansiosta TCP:n lähetysnopeus skaalautuu tehokkaasti luotettavassa verkossa, kun lähettäjän ei tarvitse jatkuvasti odottaa kuittauksia vastaanottajalta. Virheenkorjaus eli luotettava tiedonvälitys toteutetaan numeroimalla dataa järjestys- ja kuittausnumeroilla, jos vastaanottaja ei saakaan kaikkia odottamiaan datasegmenttejä se voi pyytää toista osapuolta lähettämään ne uudestaan. TCP:n tehtävä on myös järjestää väärässä järjestyksessä tulleet segmentit uudestaan oikeaan järjestykseen ennen datan välitystä sovelluskerrokselle.

+	Bitit 0-3	4-9	10-15	16-31
0	Lähdeportti		Kohdeportti	
32	Järjestysnumero			
64	Kuittausnumero			
96	Otsikon pituus	Varattu	Liput	Ikkunan koko
128	Tarkistussumma		Kiireellisyysosoitin	
160	Optiot ja täyte			
192	Data			

Kuvio 2. TCP-kehys.

Yhteydenhallinta on yksi TCP:n keskeisimmistä toiminnoista, koska pystyäkseen välittämään keskenään dataa TCP:tä käyttäen lähde- ja kohdelaitteiden pitää ensin luoda yhteys. Kun laitteet ovat lopettaneet tiedonvälityksen, ne joko lopettavat yhteyden itse tai sulkevat sen itsenäisesti ajastimen kuluessa umpeen. Yhteydenmuodostusta kutsutaan kolmivaiheiseksi kättelyksi, joka toteutetaan käyttämällä SYN- ja ACK-bittejä otsakkeen lippukentässä. Ensimmäinen osapuoli viestittää SYN-paketilla haluavansa aloittaa yhteyden, seuraavaksi toinen osapuoli lähettää SYN- ja ACK-lipuilla varustetun paketin takaisin ja viimeiseksi ensimmäinen osapuoli vielä kuittaa ACK-paketilla. Yhteys on muodostettu, ja itse dataa voidaan lähettää vasta, kun kaikki kolme vaihetta on käyty läpi. Järjestys- ja kuittausnumerot myös alustetaan satunnaisluvuilla yhteyden muodostuksen yhteydessä. Yhteyden lopetus hoidetaan käyttämällä ACK- ja FIN-lippuja, molemmat osapuolet ilmaisevat halunsa lopettaa yhteys FIN-paketilla ja kuittaavat toisen viestit ACK-paketilla. (1, s. 136—145.)

2.1.2 UDP-protokolla

UDP on yhteydetön protokolla, eli se ei muodosta yhteyttä laitteiden välille tai varmista pakettien perillemenoa päästä päähän. UDP on silti usein TCP:tä hitaampi TCP:n dynaamisen ikkunan koon ansiosta. Se sopii kuitenkin paremmin tiettyihin sovelluksiin pienemmän yleisrasitteen ansiosta, joka on yhteydettömyyden, kuittausten eliminoinnin ja kuviossa 3 esitetyn pienemmän otsakkeen ansiota. Tällaisia sovelluksia ovat muun muassa verkkopelit ja reaaliaikainen video ja ääni, joita ei haittaa yhtä paljon se, että kaikki paketit eivät tule perille joko ollenkaan tai oikeassa järjestyksessä. Segmenttien uudelleenlähetys voidaan myös toteuttaa sovellustasolla, jos sille on tarvetta. (1, s. 145.)

+	Bitit 0-15	16-31
0	Lähdeosoitteen portti	Kohdeosoitteen portti
32	Datan koko	Tarkistussumma
64	Data	

Kuvio 3. UDP-kehys perusmuodossa.

Yhteyksien multipleksointi toteutetaan TCP:ssä ja UDP:ssä samalla tavalla käyttämällä uniikkia porttia jokaiselle sovellukselle. Kun saman kerroksen protokollat kommunikoivat keskenään laitteiden välillä, porttinumero määrittää, mille sovellukselle kuljetuskerros välittää datan. Palomuurien perustoiminnallisuuden mahdollistaakin se, että jokaista saman lähde- ja kohde-IP-parin eri lähde- ja kohdeporttiyhdistelmän välistä tietovuota käsitellään erillisenä yhteytenä, näin voidaan sallia kahden laitteen välinen yksi tiettyjen sovelluksien välinen yhteys mutta estää toinen. Internet Assigned Numbers Authority eli IANA ja IETF määrittelevät niin sanotut hyvin tunnetut portit, joita tietyt sovellukset kuuntelevat, esimerkiksi TCP-portti 80 on määritelty HTTP:lle joten web-palvelimet kuuntelevat kyseistä porttia. Jos kohdelaite vastaanottaa paketin, joka on suunnattu porttiin TCP/80 ja jokin sovellus koneella kuuntelee kyseistä porttia TCP välittää paketin sisällön sille. Sovellukset voidaan toki useimmissa tapauksissa määrittää kuuntelemaan myös jotain muuta kuin sille määritettyä hyvin tunnettua porttia. (1, s. 135—140.)

2.1.3 IPv4-protokolla

Tällä hetkellä yleisimmin on käytössä IP-protokollan neljäs versio IPv4, joskin on kasvavaa painetta siirtyä IPv6:een nelosversion osoitteiden ehtymisen takia. IPv4-kehyksessä on varattu sekä lähde- että kohdeosoitteille vain 32 bittiä, mikä tarkoittaa teoriassa 2^{32} eli noin 4,3 miljardia osoitetta. Käytännössä kun tästä luvusta poistetaan osoitteet, joita ei voi reitittää julkisesti, muun muassa kokeelliset ja yksityiset osoitteet, käytettävissä on noin 3,7 miljardia osoitetta. IPv4-osoite on jaettu neljään oktettiin eli kahdeksan bitin sarjaan ja on esimerkiksi muotoa 192.168.50.5. Verkon ensimmäistä osoitetta, jonka host-bitit ovat kaikki nollia, ei voida käyttää millään päätelaitteella vaan sillä viitataan itse verkkoon esimerkiksi reititystauluissa. Verkon viimeistä osoitetta, jonka host-bitit ovat kaikki ykkösiä, ei voida myöskään käyttää. Sitä kutsutaan levitys- eli broadcast-osoitteeksi, johon lähetetyt paketit lähetetään kaikille kyseisen verkon laitteille.

+	Bitit 0–3	4–7	8–13	14-15	16–18	19–31
0	Version	Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Total Length	
32	Identifier				Flags	Fragment Offset
64	Time to Live		Protocol		Header Checksum	
96	Source IP Address					
128	Destination IP Address					
160	Options (if Header Length > 5)					
160 tai 192+	Data					

Kuvio 4. 20-tavuinen IPv4-kehys.

IP-osoitteet on alun perin jaoteltu viiteen luokkaan mutta nykyään käytetään yleisesti luokatonta järjestelmää. Osoite voidaan jakaa niin sanottuun verkko-osaan ja host-osaan, joista jälkimmäinen edustaa päätelaitteen osoitetta kyseisessä verkossa. Luokallisessa järjestelmässä luokan tunnistaa ensimmäisen oktetin arvosta ja verkko-osan voi laskea luokan perusteella, koska jokainen luokkaan kuuluva aliverkko on saman kokoinen. Taulukossa 2 on eritelty osoiteluokat ja niiden ominaisuuksia. (1, s. 107—110; 4.)

Taulukko 2. Luokalliset verkot.

Luokka	Ensimmäinen oktetti	Bittejä verkko-osassa	Verkkoja	Laitteita per verkko
A	0—127	8	126	16 777 214
B	128—191	16	16 384	65 534
C	192—223	24	2 097 152	254
D	224—239	-	-	-
E	240—255	-	-	-

Käytännössä internetin alkuaikoina A-, B- ja C-luokan verkkoja jaettiin julkiseen käyttöön, kun taas D-luokan osoitteita käytetään edelleenkin vain multicast- eli ryhmälähetysosoitteina ja E-luokka on varattu koe- ja tutkimuskäyttöön. Käytäntö huomattiin ongelmalliseksi, kun internetin kasvamisen myötä osoitteiden haaskaus tuli suuremmaksi ongelmaksi. Monille yliopistoille ja yrityksille jaettiin esimerkiksi kokonaisia A-luokan osoitteita, vaikkei millään organisaatiolla voinut olla käyttöä yli 16 miljoonalle osoitteelle. Asian ratkaisemiseksi 1990-luvulla siirryttiin luokattomaan järjestelmään, yleinen termi konseptille on Classless Inter-Domain Routing eli CIDR.

Tämä mahdollisti verkkojen jakamisen eri kokoisiin pienempiin verkkoihin, jota kutsutaan aliverkottamiseksi (engl. subnetting). Järjestelmä mahdollisti myös useiden luokallisten verkkojen yhdistämisen suuremmaksi kokonaisuudeksi, jota kutsutaan yliverkottamiseksi (engl. supernetting). (4; 5.)

Verkko- ja host-osat erotellaan 32-bittisellä verkkomaskilla, jossa on 0—32 peräkkäistä ykköstä ja loput ovat nollia. Verkkomaski ilmaistaan joko desimaalina, esimerkiksi 255.255.255.0, tai ilmoittamalla maskin ykkösten lukumäärä eli CIDR-notaationa, esimerkiksi /24. Verkko-osa saadaan selville tekemällä binäärinen AND-operaatio osoitteen ja maskin kesken, operaatio on havainnollistettu alla.

Osoite:		11000000.10101000.00110010.00000101 (192.168.50.5)
Verkkomaski:		11111111.11111111.11111111.00000000 (255.255.255.0)
	AND	
Verkko:		11000000.10101000.00110010.00000000 (192.168.50.0)
Levitysosoite:		11000000.10101000.00110010.11111111 (192.168.50.255)

A-luokan osoitteiden oletusverkkomaski on aina 255.0.0.0, B-luokan 255.255.0.0 ja C-luokan 255.255.255.0. Luokallisessa järjestelmässä verkko voidaan myös aliverkottaa jollain muullakin maskilla mutta jokaisen kyseisen luokan aliverkon täytyy tällöin käyttää samaa maskia. Luokattomassa järjestelmässä luokallisen verkon voi aliverkottaa niin monella eri verkkomaskilla kuin on tarpeen.

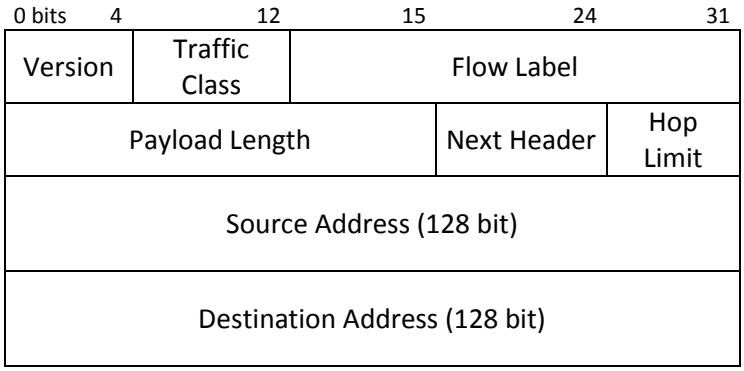
IPv4-osoitteiden loppumista on ennustettu jo pitkään mutta erilaisten teknologioiden käyttöönotto on tuonut helpotusta ongelmaan. Luokattoman aliverkotuksen lisäksi osoitteenmuunnostekniikka Network Address Translation eli NAT ja yksityiset IP-osoitteet ovat auttaneet eniten osoitteiden säästämisessä. RFC 1918 määrittää A-, B- ja C-luokista jokaisesta yhden osion yksityisille osoitteille, joita voidaan käyttää vain organisaatioiden sisällä, eli niitä ei reititetä internetissä (6, s. 552). Käyttämällä sisäisesti yksityisiä osoitteita isokin organisaatio voi pärjätä vain muutamalla julkisella IP-osoitteella muuntamalla internetiin menevältä liikenteeltään lähdeosoitteen johonkin organisaation käytössä olevaan julkiseen osoitteeseen. Käyttämällä porttimuunnos-tyyppistä NAT:a periaatteessa yli 65000 sisäverkon laitetta voi käyttää samaa julkista osoitetta monta yhteen periaatteella, jolloin sisäverkon laitteiden yhteydet internetiin

yksilöidään porttinumeroilla. Palvelimien tapauksessa, jottei osoite muuttuisi, käytetään usein staattista NAT:a, jolloin tietty yksityinen osoite muunnetaan aina tiettyyn julkiseen osoitteeseen yksi yhteen -periaatteella. Hieman vähemmän käytetty osoitteenmuunnostyyppi on dynaaminen NAT, jossa reunareitittimelle on määritetty tietty määrä julkisia IP-osoitteita. Niitä otetaan käyttöön internetiin meneville yhteyksille sitä mukaa kun tarvetta syntyy. Rajoittava tekijä dynaamisessa NAT:ssa on julkisten osoitteiden määrä, jos kaikki julkiset osoitteet ovat käytössä, kukaan muu ei enää pääse internetiin. (6, s. 553—558.)

2.1.4 IPv6-protokolla

IP-protokollan seuraavaa versiota IPv6:a alettiin kehittämään jo melko varhain 1990-luvun alussa kun nähtiin että IPv4-osoitteet eivät tule riittämään loputtomiin. Uudessa versiossa tähän varauduttiin hyvin määrittämällä osoitteen pituudeksi 128 bittiä, joka antaa 2^{128} eli noin 3,4 x 10^{38} mahdollista osoitetta. IPv6-osoitteet esitetään heksadesimaalimuodossa ja ne ovat esimerkiksi muotoa 2001:3A::5C0:6C0A:101. Osoite on jaettu kahdeksaan 16 bitin sarjaan, jotka erotetaan kaksoispisteillä. Peräkkäiset nollasarjat voidaan lyhentää kerran osoitteessa ::-merkinnällä ja sarjojen aloittavat nollat voidaan jättää pois. Verkko-osa ilmoitetaan yksinomaan CIDR-notaationa, esimerkiksi /64. (6, s. 580—581; 7.)

Suuren osoiteavaruuden ansiosta voidaan unohtaa NAT, joka on ongelmallinen joillekin sovelluksille, jotka vaativat suoraa päästä päähän -yhteyttä. Kuviossa 5 esitettyä otsaketta on myös paranneltu poistamalla turhiksi tai vähän käytetyksi havaittuja kenttiä ja lisäämällä joitakin uusia. Esimerkiksi tarkistussumma-kenttä on eliminoitu kokonaan IPv6:ssa, ja eri tietovuot voidaan merkitä Flow Label -arvolla. Peruskerroksen protokollat, kuten Ethernet, tosin silti käyttävät tarkistussummaa yleisesti omissa otsakkeissaan. Flow Labelin käyttö mahdollistaa nopeamman tiedonsiirron siten, että reitittimien tarvitsee käsitellä kokonaan vain merkityn vuon ensimmäisen paketin otsakkeet ja kirjoittaa tulos välimuistiin. Vuon seuraavat paketit voidaan reitittää nopeasti eteenpäin samaa reittiä lukemalla vain ohjeet välimuistista. Internetin tietoturva-arkkitehtuuri IPsec on myös pakollinen IPv6:ssa toisin kuin IPv4:ssä, jossa jokaisen laitteen ei ollut pakko tukea sitä. (6, s. 580—581; 7.)



Kuvio 5. 40-tavuinen IPv6-kehys.

IPv6:een siirtyminen tulee olemaan suurimmaksi osaksi hidas prosessi, koska se ei ole yhteensopiva IPv4:n kanssa. Siirtymän helpottamiseksi on kehitetty useita standardeja, joista tärkeimpiä ovat niin sanottu dual stack ja tunnelointi. Dual stack -konfiguraatiolla tarkoitetaan tilannetta jossa päätelaite tukee sekä IPv4:ää että IPv6:tta ja sille on määritelty osoite molemmista protokollista. Useimmat käyttöjärjestelmät pyrkivät käyttämään IPv6:tta oletuksena mutta siirtyvät IPv4:ään jos IPv6-yhteys ei toimi. Tunnelointitekniikat yleensä toteutetaan verkkojen reunalla sijaitsevissa reitittimissä, poikkeuksena Teredo-tunnelit joiden avulla päätelaite voi luoda tunnelin suoraan toiseen päätelaitteeseen. 6to4-tunneloinnissa IPv6-paketit enkapsuloidaan IPv4-pakettien sisään jolloin IPv6-natiivit laitteet voivat kommunikoida suoraan IPv4-verkon ylitse. Intra-Site Automatic Tunnel Addressing Protocol eli ISATAP taas on tarkoitettu IPv6-liikenteen tunnelointiin organisaation sisällä, ISATAP-tunnelien yhteensopimattomuus IPv4 NAT:n kanssa rajoittaa tekniikan käyttöä. (6, s. 609—611; 8.)

2.2 OSI-malli

OSI eli Open Systems Interconnection -malli on 1970-luvun lopussa ISO:n eli International Standards Organizationin kehittämä tietoverkkojen kommunikaatiomalli. Internetin alkutaipaleella oli muitakin kilpailevia malleja, joista loppujen lopuksi TCP/IP vei voiton yleistyen maailmanlaajuisesti. Tarkasti OSI-mallia käyttäviä tietokoneita ei todennäköisesti enää löydy mistään, mutta mallia käytetään yleisesti koulutuskäytössä ja keskustelussa käsitetasolla, koska muita malleja ja protokollapinoja voidaan helposti esittää OSI-mallin kautta. Taulukko 3 esittää OSI-mallin kerrokset, jotka ovatkin pitkälti saman nimisiä TCP/IP-mallin kerrosten kanssa. (6, s. 32.)

Taulukko 3. OSI-mallin kerrokset ja vastaavia protokollia.

7. Sovelluskerros	HTTP, FTP, SMTP
6. Esitystapakerros	GIF, JPG, MPEG
5. Istuntokerros	AppleTalk, WinSock
4. Kuljetuskerros	TCP, UDP
3. Verkkokerros	IP, ICMP, IPX
2. Siirtokerros	Frame Relay, Ethernet
1. Fyysinen kerros	Ethernet, Token Ring

TCP/IP-mallia verrataan yleisesti OSI-malliin, koska molempien mallien kerrokset vastaavat hyvin toisiaan. Esimerkiksi IP:stä puhutaan kolmannen kerroksen eli Layer 3 tai L3-protokollana, koska se vastaa OSI-mallin verkkokerrosta, vaikka se onkin TCP/IP-mallissa toisen kerroksen protokolla. Kuvio 6 havainnollistaa, mitkä TCP/IP:n kerrokset vastaavat mitäkin OSI-mallin kerroksia.

Kuvio 6. TCP/IP-mallin kerrosten sijoittuminen OSI-mallissa.

Nykyteknologian puitteissa OSI-mallista tärkeimpiä sen seuraajille perittyjä käsitteitä ovat kerrosten erikoistuminen tiettyihin tehtäviin ja tarve kerroksia erottaville rajapinnoille.

3 Palomuurit

Internetin kasvaessa 1980-luvulla tietoturvaan alettiin kunnolla kiinnittää huomiota vasta, kun ensimmäiset tietoturvahyökkäykset tulivat ilmi. Marraskuussa 1988 Morris-mato alkoi levitä internetissä saastuttaen muun muassa yliopistojen ja NASA:n tietoverkkoja pakottaen kehittäjät ja tutkijansa siihen todellisuuteen, että internet ei ollut enää vain heidän oma suljettu yhteisönsä. Tämä johti internet-yhteisössä kasvaneeseen keskusteluun tietoturvasta ja esimerkiksi ensimmäisen CERT-

organisaation eli Computer Emergency Response Teamin perustamiseen. CERT luotiin vastaamaan muun muassa tietoturvauhkien ennaltaehkäisystä, havainnoinnista, tiedottamisesta ja ratkaisusta (10). Nykyään monella valtiolla on oma kansallinen CERT-organisaationsa, esimerkiksi Suomessa CERT-FI. (9.)

Morris-mato oli pelkkä opiskelijan liikkeelle laskema kokeilu mutta tietoturvauhat muuttuivat ajan myötä vakavemmiksi rikollisten siirtyessä internetiin, kun hakkeroinnilla alkoi olla mahdollista ansaita rahaa. Palomuurien kehitys ja myynti lähti myös kunnolla käyntiin, kun hyökkäykset alkoivat 1990-luvulla yleistyä ja niistä tiedotettiin laajemmin myös julkisuudessa. Nykyään suurimpia palomuurien valmistajia ovat muun muassa Cisco, Juniper Networks, Check Point ja Fortinet. (9.)

3.1 Palomuurien ominaisuuksia ja historiaa

Palomuuri on joko erillinen laite tai ohjelmisto, jonka tarkoitus on kontrolloida ja valvoa verkon liikennettä ja toteuttaa sille määriteltyä tietoturvapolitiikkaa. Monissa reittimissäkin on joitakin palomuuritoimintoja, toisaalta monet palomuurit pystyvät myös tekemään perusreititystä. Palomuurit voidaan jakaa kahteen eri tyyppiin eli verkko- (engl. network firewall) ja päätelaitepalomuureihin (engl. host firewall). Verkkopalomuuri on yleensä erillinen laite, joka on kytketty tietoverkkoon tarkoituksena kontrolloida pääsyä yhteen tai useampaan päätelaitteeseen tai verkkoon. Päätelaitepalomuuri on yleensä ohjelmisto, joka suojaa vain sitä tietokonetta, johon se on asennettu. Molempia palomuurityyppejä käytetään yleisesti samanaikaisesti tietoturvan lisäämiseksi. Päätelaitteissa sijaitsevat palomuurit pystyvät myös valvomaan salattua liikennettä, koska salaus puretaan samassa päätelaitteessa, toisin kuin verkkopalomuurit, joiden läpi kyseinen liikenne kulkee vielä salattuna. Työssä käsitellään tästä eteenpäin pelkästään verkkopalomuureja. (14.)

Käsitetasolla palomuurin on tarkoitus olla pullonkaula kahden tai useamman verkon välissä, jonka läpi kaikki verkkojen välinen liikenne menee. Näin sen avulla liikennettä voidaan kontrolloida ja siitä voidaan pitää kirjaa eli lokeja. Palomuuri määrittää, mikä liikenne on sallittua ja mikä kiellettyä tarkastelemalla pakettien ominaisuuksia. Nykyiset kehittyneemmät yrityskäyttöön suunnatut palomuurit pystyvät tekemään muitakin toimintoja, kuten virustorjuntaa, tunkeutumisen havaitsemista, liikenteen salausta,

osoitteenmuunnosta ja liikenteen priorisointia. Virustorjuntaa toteutetaan tutkimalla paketteja sovellustasolla ja vertaamalla dataa virustietokantoihin. Tunkeutumisen havaitsemista (Intrusion Detection System eli IDS) ja murron estämistä (Intrusion Prevention System eli IPS) toteutetaan tutkimalla paketit ja tietovuot sovellustasolla verraten niitä tunnettuihin hyökkäyksiin ja hyökkäyskuvioihin.

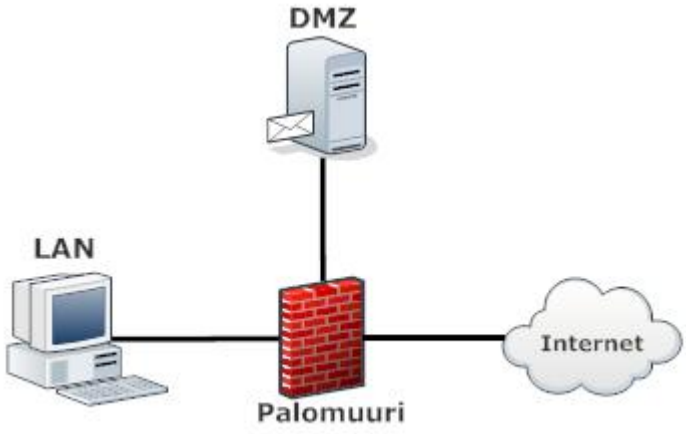
Liikenteen salausta kutsutaan VPN- eli Virtual Private Network -teknologiaksi ja loogisia VPN-yhteyksiä kutsutaan tunneleiksi. VPN-teknologialla esimerkiksi kaksi tai useampia yrityksen verkkoja voidaan yhdistää julkisessa verkossa muodostaen yksityisen verkon. Yksittäisiä etätyöntekijöitä voidaan myös yhdistää yrityksen verkkoon internetin kautta tietoturvallisesti VPN-tunnelien avulla. Edellisessä tapauksessa palomuurit toimivat VPN-tunnelin päätepisteinä, ts. tunneli terminoidaan kyseisiin palomuureihin. Etäkäyttö-VPN:ssä käyttäjä muodostaa tunnelin palomuuriin omasta tietokoneestaan VPN-ohjelmistolla. Taatakseen riittävän tietoturvan tunnelin muodostavien osapuolten tulee varmistaa tunnelin luottamuksellisuus, toisen osapuolen henkilöllisyys ja datan eheys. VPN-tunnelit toteutetaan pääosin IPsec-arkkitehtuurilla, joka pitää sisällään useita eri protokollia edellisten vaatimusten täyttämiseksi, käytettävät protokollat sovitaan tunnelia muodostettaessa. Yksityisyys varmistetaan salaamalla liikenne jollakin salausprotokollalla kuten AES tai 3DES. Toinen osapuoli todennetaan joko ennalta määritellyllä avaimella tai digitaalisella sertifikaatilla. Datan eheys todennetaan niin, että lähettäjä laskee datasta tiivisteen hash-algoritmillä, kuten MD5:llä tai SHA:lla, ja sisällyttää sen otsakkeeseen. Saadessaan paketin vastaanottaja laskee tiivisteen uudestaan samalla algoritmillä. Jos data on jostakin syystä muuttunut matkalla, niin vastaanottajan laskema tiiviste ei ole sama kuin lähettäjän, tällöin vastaanottaja voi hylätä paketin sen oletuksen perusteella, että kolmas osapuoli on muuttanut dataa matkalla. (6, s. 528—536.)

Osoitteenmuunnosta eli NAT:a, joka on määritelty RFC 3022:ssa, tehdään yleisimmin yksityisen ja julkisen verkon reunalla sijaitsevassa reitittimessä tai palomuurissa. Muuntamalla sisäverkon yksityisiä osoitteita julkisiin osoitteisiin organisaatio voi säästää rajallisia julkisia IP-osoitteitaan ja luoda ylimääräisen tietoturvakerroksen sisäverkon suojaksi, koska NAT piilottaa sisäverkon osoiteavaruuden ulkopuolisilta. Käytännössä NAT:ia tekevä laite voi uudelleenkirjoittaa sisään- ja ulostulevien pakettien lähde- ja kohdeosoitteita ja portteja laitteeseen määriteltyjen sääntöjen mukaisesti. Laite pitää

kirjaa tekemistään osoitteenmuunnoksista taulun muodossa, johon merkitään vähintään alkuperäinen osoite ja uudelleenkirjoitettu osoite. Alkio poistetaan taulusta, kun yhteys lopetetaan tai sitä ei ole käytetty tiettyyn aikaan. Alkuperäistä osoitetta kutsutaan usein joko sisäiseksi tai lokaaliksi osoitteeksi ja uudelleenkirjoitettua osoitetta joko ulkoiseksi tai globaaliksi osoitteeksi. (6, s. 553.)

Liikenteen priorisointiin viitataan yleisesti termillä QoS eli Quality of Service, suomeksi palvelun laatu. QoS:ää voidaan toteuttaa esimerkiksi IPv4-otsakkeen 6-bittisellä DSCP- eli Differentiated Services Code Point -kentällä. Liikennettä voidaan luokitella muun muassa sovellusten, käyttäjien ja lähde- tai kohdeverkkojen mukaan. Reititin tai palomuuri voi priorisoida liikennettä QoS-luokkien perusteella, jos linkki on ruuhkainen. Liikenne, jolla on pienempi prioriteetti, joutuu odottamaan lähetysvuoroaan kauemmin ruuhkaisella linkillä tai se voidaan pudottaa kokonaan. On myös mahdollista määritellä, että tietylle luokalle taataan tietty määrä kaistaa linkillä. QoS:ää käytetään yleensä suurempien organisaatioiden sisäverkoissa varmistamaan, että aikakriittinen tai muuten tärkeä liikenne, kuten VoIP, ei kärsi jos verkossa on ruuhkaa. (16.)

Tyypillisin paikka palomuurille on sisäisen verkon eli LANin ja internetin rajalla, joka on usein tietoturvan kannalta kriittisin piste. Organisaation ulkoisia palveluita tarjoavien laitteiden, kuten sähköpostipalvelimien on oltava saavutettavissa myös internetistä, joten ne sijoitetaan omaan verkkoonsa, jota kutsutaan demilitarisoiduksi alueeksi (engl. demilitarized zone eli DMZ). Kaikki demilitarisoidulle alueelle tuleva ja sieltä lähtevä liikenne kulkee palomuurin kautta. DMZ lisää ylimääräisen tietoturvatason lähiverkkoon, koska alueen tietoturvapolitiikan on oltava avoimempi on verkko myös avoimempi hyökkäyksille. Hyökkäyksen onnistuessa vahinko on rajattu DMZ-verkkoon, koska tyypillisen tietoturvapolitiikan mukaan DMZ:stä ei voi ottaa suoria yhteyksiä lähiverkkoon. Kuviossa 7 on havainnollistettu, kuinka kaikki näiden kolmen verkkosegmentin yhteydet kulkevat saman palomuurin kautta. (6, s. 158.)



Kuvio 7. Tyypillinen yksinkertaistettu verkkotopologia organisaation verkon reunalla.

Toinen tyypillinen paikka, mihin palomuureja sijoitetaan, on sisäverkossa erilaisten verkkosegmenttien välissä. Tämä johtuu usein siitä, että eri segmenteillä on erilaiset tietoturvatasot, esimerkiksi vierailijaverkosta ei yleensä tarvitse päästä henkilöstöosaston verkkoon. Sijoittamalla palomuureja sekä verkon reunalle että sisäverkkoon voidaan myös luoda ylimääräisiä tietoturvakerroksia. Tietoturvaa verrataankin usein sipuliin, läpäistyään tai ”kuorittuaan pois” yhden kerroksen mahdollinen hyökkääjä saisi vain vastaansa uuden kerroksen. (15.)

Pakettisuodatinpalomuuri

Ensimmäisen sukupolven palomuurit 1980-luvun lopulla olivat yksinkertaisia tilattomia pakettisuodattimia (engl. packet filter). Nämä palomuurit tarkastelevat paketteja lähde- ja kohdeosoitteiden ja porttinumeroiden perusteella eli ne toimivat pääasiassa OSI-mallin kolmella alimmalla kerroksella, kuljetuskerrokselta tarkastellaan vain porttinumeroita. Jokaista pakettia verrataan palomuurin säännöstöön, jos paketti vastaa johonkin sääntöön se joko sallitaan, kielletään tai hylätään. Kielletyt paketit pelkästään pudotetaan eli niihin ei vastata eikä niitä välitetä eteenpäin, hylätyt paketit pudotetaan ja palomuuri myös informoi lähdelaitetta asiasta ICMP-paketilla. (11.)

Pakettisuodatinpalomuurit ovat tilattomia, joka tarkoittaa sitä, että ne eivät kiinnitä huomiota siihen onko tarkasteltava paketti jonkin olemassaolevan tietovuon osa. Tilaton palomuuri ei siis pidä kirjaa kuljetuskerroksen yhteyksistä tai niiden tiloista, jonka johdosta jokaista pakettia on pakko verrata säännöstöön, että voidaan määrittää

mitä sille pitäisi tehdä. Tilaton palomuuri soveltuu hyvin verkkoon, jossa on vain yksinkertaisia liikennekuvioita eli tiedetään tarkasti esimerkiksi, mitä portteja verkossa liikennöivät sovellukset käyttävät. Monien protokollien paluupakettien portteja ei voida tietää etukäteen, koska ne valitaan dynaamisesti. Tällaisten sovellusten toimivuuden varmistamiseksi voidaan joutua avaamaan esimerkiksi kaikki niin sanotut yläportit eli portit väliltä 1024—65535, joiden joukosta dynaamiset portit valitaan. Tällaisten ylimääräisten porttien avaamisten ansiosta sisäverkko on luonnollisesti haavoittuvaisempi hyökkäyksille. (9; 11.)

Ensimmäiset pakettisuodatinpalomuurit olivat usein reitittimiä, joissa toiminta perustui pääsylistoihin eli ACL:iin (engl. Access Control List). Reitittimessä voitiin esimerkiksi määrittää, että tietyn verkkosovittimen sisäänpäin tulevaa liikennettä verrataan tiettyyn pääsylistaan. Listaa käydään läpi järjestyksessä ylhäältä alas, ja kun paketti vastaa johonkin sääntöön prosessointi loppuu ja paketti käsitellään säännön mukaan, eli jokaista sääntöä ei käydä välttämättä läpi. Pääsylistassa on viimeisenä aina oletussääntö, joka kieltää kaikki paketit. Kaikki liikenteen sallivat säännöt on siis tarkoitus sijoittaa ennen oletussääntöä. Tämä havainnollistaa hyvin palomuurien yleistä toimintaperiaatetta, eli ”kaikki liikenne, jota ei erikseen sallita, on kielletty”. (9; 11.)

Tilallinen palomuuri

Pakettisuodatinpalomuurien kehitys jatkui ja 1990-luvun puolivälissä markkinoille tuli tilallisia palomuureja, jotka toimivat muuten samalla pakettisuodatusperiaatteella, paitsi ne myös pitävät kirjaa niiden läpi kulkevista yhteyksistä. Tilallinen palomuuri siis toimii OSI-mallin neljännellä eli kuljetuskerroksella, mukaan lukien alemmat kerrokset. Kun palomuuri näkee, että uusi TCP-yhteys avataan tutkitaan ensin onko yhteys sallittu säännöstön mukaan ja jos yhteys sallitaan se kirjataan yhteystauluun. Yhteydettömät protokollat, kuten UDP, kirjataan myös yhteystauluun. Tällöin palomuurien yhteydessä puhutaan UDP-yhteyksistä, vaikka UDP onkin yhteydetön protokolla. Seuraavien pakettien kohdalla tutkitaan ensin, ovatko ne osa jotakin olemassaolevaa yhteyttä, ja jos ne ovat, niin ne sallitaan suoraan. Paketteja siis tutkitaan säännöstöä vastaan vain, jos ne eivät ole osa jotakin olemassa olevaa yhteyttä. (11.)

Yhteystauluun tyypillisesti tallennetaan mahdollisimman paljon yhteyksiä yksilöiviä tietoja, esimerkiksi:

- uniikki tunniste yhteydelle palomuurin sisäiseen käyttöön
- yhteyden tila eli esimerkiksi kättely, muodostettu tai suljettava
- TCP-yhteyksissä järjestysnumero
- lähdeosoite
- kohdeosoite
- fyysinen verkkosovitin josta paketit saapuvat
- fyysinen verkkosovitin josta paketit lähtevät.

Yhteys poistetaan yhteystaulusta, kun palomuuri näkee, että se suljetaan, tai kun se on ollut käyttämättömänä tarpeeksi kauan. Yhteyden sulkemisen jälkeen yhteyteen kuuluvia paketteja ei enää päästetä läpi. UDP-yhteydet poistetaan aina yhteystaulusta vasta, kun niiden aikaraja umpeutuu, tämän takia aikarajat on syytä asettaa huolella. Jos yhteydet vanhentuvat liian hitaasti, yhteystaulu voi esimerkiksi palvelunestohyökkäyksen aikana kasvaessaan viedä niin paljon muistia, että palomuuri ei pysty enää prosessoimaan normaalia liikennettä. (12.)

Yhteyksien seuraaminen mahdollistaa sen, että tilallinen palomuuri osaa käsitellä liikennettä myös hieman älykkäämmin. Tilattomaan palomuuriin on pakko konfiguroida kaksi erillistä sääntöä saman yhteyden molempiin suuntiin kulkevalle liikenteelle. Nähdessään, että palomuurille saapuva paketti on osa jotakin olemassaolevaa yhteyttä, tilallinen palomuuri voi sallia liikenteen pelkästään yhden säännön perusteella. Tarkemmin sanottuna kumpaan suuntaan tahansa menevät paluupaketit sallitaan aina ilman erillistä sääntöä, tämän ansiosta palomuuriin ei tarvitse esimerkiksi avata yhtään ylimääräistä porttia kyseisen liikenteen mahdollistamiseksi.

Sovelluspalomuuri

Kolmannen sukupolven palomuurit pystyivät jo tarkastelemaan liikennettä OSI-mallin seitsemännellä kerroksella eli sovelluskerroksella. Ensimmäinen sovelluspalomuuri tuli markkinoille jo vuonna 1991, kun Digital Equitpment Corporation esitteli SEAL-palomuurin, joka käytti protokollakohtaisia välityspalvelimia eli proxyjä liikenteen tarkastamiseen. Sovelluspalomuurit pysyivät erillisinä ja erikoistuneina tuotteina melko

pitkälle mutta teknologian kehityttyä niiden toiminnallisuudet integroitiin pitkälti niin sanottuihin tavallisiin palomuureihin. Useimmat nykyaikaiset yrityskäyttöön tarkoitetut palomuurit ovatkin tilallisen ja sovelluspalomuurin yhdistelmiä. (12.)

Sovelluspalomuurin suurin etu on, että se pystyy ymmärtämään tiettyjä sovelluksia ja protokollia, kuten FTP, HTTP ja telnet. Pakettien sovellustason tarkastelu (engl. deep inspection) toteutetaan edelleenkin usein palomuurin sisäisten välityspalvelimien tai erikoistuneiden sovelluskohtaisten ohjelmien avulla. Tarkkailemalla paketin sisältämää dataa palomuuri voi esimerkiksi tunnistaa FTP-komentoja ja pudottaa paketin, jos se näkee laittoman komennon. Toisin kuin verkkotasolla toimiva pakettisuodatinpalomuuri, sovelluspalomuuri voi myös tunnistaa ja kieltää haitallisen liikenteen kuten tietyn koodinpätkän, joka käyttää muuten sallittua protokollaa tai porttia tai molempia. Tarkastelemalla pakettien sisältöä voidaan myös sallia liikennettä ja avata uusia portteja esimerkiksi lukemalla FTP-hallintaviesteistä, mitä dynaamista porttia FTP-datakanava tulee käyttämään. (12; 13.)

Tutkiessaan pakettien sisältöä näin yksityiskohtaisesti sovelluspalomuuri toimii pitkälti samalla tavalla kuin murron estämisjärjestelmä eli IPS, koska molemmat voivat verrata liikennettä tiettyihin kuvioihin, jotka vastaavat tunnettuja verkkohyökkäyksiä. IPS:t saavuttavat tosin parempia ja tarkempia tuloksia vertaamalla sen hetkisiä liikennekuvioita normaaliksi määriteltyihin kuvioihin ja korreloimalla pidemmältä ajalta tai useammasta paketista kerättyjä tietoja. (13.)

3.2 StoneGate-palomuuriratkaisu

StoneGate on suomalaisen tietoturvayhtiö Stonesoftin vuonna 2001 julkaisema kokonaisvaltainen verkkotietoturvaratkaisu. Stonesoft perustettiin vuonna 1990, ja yhtiö listautui Helsingin pörssiin vuonna 1999. Toimitusjohtajana toimii yhtiön perustaja Ilkka Hiidenheimo. Yhtiöllä oli vuoden 2010 lopussa henkilökuntaa noin 200, pääkonttori Helsingin Lauttasaaressa, alueellinen päätoimisto Yhdysvaltojen Atlantassa ja tutkimus- ja kehitystoimintoja Etelä-Ranskassa. Yhtiö toimii globaalisti, joten sillä on myös useita kymmeniä pienempiä myyntitoimistoja ympäri maailmaa. Liikevaihto oli vuonna 2010 noin 24 miljoonaa euroa. Liikevoitto oli jo kymmenennettä peräkkäistä vuotta tappiollinen mutta yhtiö on kasvu-uralla kasvattaen vuoden 2011 kolmannella

neljänneksellä tuotemyyntiään 60 % verrattuna edellisen vuoden vastaavaan ajanjaksoon. (17; 18; 19.)

Stonesoft esitteli vuonna 1994 StoneBeatin, joka oli ohjelmistopohjainen teknologia palomuurien klusterointiin. StoneBeat-tuoteperhettä laajennettiin vuonna 1999 StoneBeat FullCluster -tuotteella, joka mahdollisti muun muassa Check Point FW-1 -palomuurien vikasietoisen klusteroinnin ja kuormantasauksen klusterin jäsenten kesken. Yhtiö teki Check Pointin kanssa tuotteen tiimoilta tiivistä yhteistyötä ja StoneBeat FullCluster olikin ensimmäisiä Check Pointin OPSEC-ohjelmassa sertifioituja teknologioita. Stonesoft siirtyi lopulta pelkästä ohjelmistotalosta palomuurien valmistajaksi ja Check Pointin suoraksi kilpailijaksi vuonna 2001 julkaistun StoneGate Firewall/VPN -palomuurin myötä. (20.)

StoneGate-palomuuri on yksi osa StoneGate-tietoturvaratkaisua, joka on erityisesti suunniteltu monimutkaisiin ja hajautettuihin verkkoympäristöihin. StoneGate tarjoaa palomuuri- ja VPN-palveluiden lisäksi myös murron havaitsemista ja estämistä StoneGate IPS -ratkaisun avulla. Palomuurit ja IPS:t toimivat myös yhdessä ilman valvontaa, IPS voi esimerkiksi havaitessaan hyökkäyksen laittaa käyttäjän mustalle listalle ja pyytää saman toimipaikan palomuurejakin estämään kyseiset yhteydet määräajaksi. StoneGate-palomuurit pystyvät myös tutkimaan liikennettä ja estämään hyökkäyksiä kuten IPS:t, tosin vain suppeammassa mittakaavassa, koska tutkinnalle voidaan omistaa palomuurissa vain rajattu määrä laitteen resursseista. (22.)

Yksi StoneGate-ratkaisun vahvuuksista on, että kaikkia komponentteja ja konfiguraatioita hallitaan keskitetysti saman järjestelmän, StoneGate Management Centerin eli SMC:n, kautta. Koko järjestelmä on myös suunniteltu ja rakennettu alusta alkaen keskitetysti hallittavaksi ja valvottavaksi sen sijaan, että hallintajärjestelmä olisi vain liimattu päälle jälkikäteen. Palomuurit ja IPS:t onkin integroitu hyvin tiiviisti SMC:hen, eikä niitä käytännössä voi ottaa käyttöön tai hallita ilman toimivaa SMC-palvelinta. (22.)

StoneGate-palomuuri on tyypiltään tilallinen sovelluspalomuuri, kaikki paitsi nykyisen malliston pienin malli tarjoavat myös lisenssinvaraisia UTM eli Unified Threat Management -ominaisuuksia. UTM yhdistää palomuuriin muitakin perinteisiä

tietoturvateknologioita, kuten IPS-toimintoja, virustorjuntaa, web-suodatusta ja roskapostin suodatusta. Palomuuri toimii tietoturvallisemmaksi kustomoidun Debian Linux -käyttöjärjestelmän päällä. Ylläpitäjien ei tosin tarvitse viettää paljoa aikaa palomuurin komentorivillä, ja kaikki tarpeelliset käyttöjärjestelmän päivityksetkin tulevat palomuuriohjelmiston päivitysten mukana. (22.)

Klusterointi on rakennettu sisään StoneGate-palomuurien toimintaan eli se ei tarvitse erillisiä laitteita tai ohjelmistoja. Klusteroinnin avulla 2—16 palomuuria voivat toimia yhtenä loogisena kokonaisuutena. Koska palomuuri yleisesti sijoitetaan tietoliikenteen solmukohtaan, se estää kaiken liikenteen kulun rikkoontuessaan tai saadessaan toimintahäiriön. Klusteroinnilla päästään eroon näistä yhden laitteen häiriöistä (engl. single point of failure) koska yhden klusterin jäsenen mennessä rikki, muut jäsenet silti hoitavat liikennettä. Huoltokatkojen vaikutus voidaan näin ollen myös minimoida, koska klusterin jäsenet voidaan ottaa pois käytöstä yksi kerrallaan esimerkiksi päivityksiä varten. Klusterointiasetukset määritetään SMC:ssä, ja näistä asetuksista ehkä tärkein on, toimiiko klusteri valmiustilassa (standby) vai kuormanjakotilassa (load balancing). Valmiustilassa yksi laite on aktiivisena hoitamassa liikennettä, ja loput laitteet ovat varalla, jos aktiivinen laite ei pysty enää käsittelemään liikennettä. Kuormanjakotilassa kaikki laitteet hoitavat samaan aikaan yhdessä liikennettä, ja se onkin kustannustehokkain ja suositelluin tapa klusteroida laitteita. (22.)

Klusterin jäsenten välinen kommunikaatio on klusterin toiminnalle elintärkeää. Klusterin jäsenet kommunikoivat keskenään erikseen määritellyn heartbeat-verkon välityksellä käyttäen ryhmälähetysosoitteita, joita kaikki klusterin jäsenet kuuntelevat. Heartbeat-verkossa vaihdetaan tietoa avoimista yhteyksistä state sync -yhteyden avulla ja palomuurien tiloista heartbeat-yhteyden avulla. Koska yhden yhteyden eri paketit voivat kulkea usean eri klusterin jäsenen läpi, jokaisella jäsenella on oltava tiedot kaikista klusterin läpi kulkevista yhteyksistä. Jos klusterin jäsenet eivät tiedä toistensa käsittelemiä yhteyksiä, yhteyttä käsittelevän laitteen rikkoutuessa yhteys katkeaisi, koska muut laitteet eivät tietäisi sen olemassaolosta. Heartbeat-liikenteen avulla klusterin jäsenet tietävät toisten jäsenien tilan ja joitakin muita tietoja kuten niiden ohjelmistoversion. Heartbeat-viestejä lähetetään oletuksena sekunnin välein, ja jos joltakin jäseneltä ei nähdä heartbeat-paketteja viiteen sekuntiin, muut jäsenet olettavat, että se on poissa käytöstä. Heartbeat-daemonin todetessa toisen jäsenen

olevan poissa käytössä se poistetaan väliaikaisesti klusterista. Klusterin ollessa valmiustilassa jokin varalla oleva jäsen aktivoituu, kun taas kuormantasaustilassa jäljellä olevat laitteet jatkavat liikenteen käsittelyä. (22.)

Pakettien sovellustason tarkastelu mahdollistaa StoneGate-palomuureissa myös liikenteen tarkemman luokittelun ja suodatuksen. Palomuuri pystyy esimerkiksi tutkimaan HTTP-paketeista URL-osoitteita ja estää pääsyn tiettyihin osoitteisiin tai tiettyyn kategoriaan, kuten viihteeseen liittyville sivuille. StoneGate-palomuurin ohjelmistoon on sisällytetty sama tietokanta tunnetuista hyökkäyksistä kuin StoneGate IPS-laitteisiin, joten palomuuri voi myös tutkia tiettyjä protokollia tarkemmin tietokantaa vasten. Toisin kuin IPS-laitteet, jotka pystyvät tutkimaan miltei kaikkia protokollia, palomuuri on rajoitettu kuuteen protokollaan, jotka ovat HTTP, HTTPS, IMAP, POP3, SIP ja SMTP. Liikenteen vastatessa jonkin tunnetun hyökkäyksen kuviota se voidaan joko sallia, pysäyttää tai keskeyttää. (22.)

Yksi StoneGate-palomuurien erikoisuus on Stonesoftin kehittämä ja patentoima Multi-Link-teknologia, joka mahdollistaa usean internet-yhteyden käytön ilman erillisiä protokollia. On olemassa kaksi eri Multi-Link-tilaa, joita voidaan käyttää myös samanaikaisesti eri internet-yhteyksissä. Kuormantasaustilassa eri yhteyksiä kuormitetaan joko niiden sen hetkisen nopeuden tai käsin määritetyn kaistamäärän perusteella. Valmiustilassa yksi tai useampi yhteys on varalla, jos ensisijainen yhteys ei toimi. (22.)

StoneGate-palomuuria myydään valmiina fyysisenä laitteena, virtuaalikoneena ja pelkkänä ohjelmistona, joka on tarkoitettu ajettavaksi erillisellä palvelimella. Valmiita laitteita, joiden ominaisuuksia on esitelty taulukossa 4, on tarjolla pienistä pöytämallisista laatikoista lähtien kolmen räkkiyksikön kokoisiin laitteisiin asti. Pienimmät laitteet, kuten FW-105 ja FW-315, on tarkoitettu pieniin etätoimistoihin, keskikokoiset FW-1060 ja FW-1301 suurempiin päätoimipaikkoihin ja kaikkein suurimmat laitteet esimerkiksi operaattorikäyttöön. Laitteista on myös tarjolla muutama muu niin sanottu välimalli, joita kaikkia ei ole merkitty taulukkoon.

Taulukko 4. StoneGate-palomuurimallien ominaisuuksia (23).

Laitemalli	FW-105	FW-315	FW-1060	FW-1301	FW-3201	FW-5201
Suoritusteho	100 Mbps	500 Mbps	1,6 Gbps	5 Gbps	10 Gbps	20 Gbps
VPN-suoritusteho	25 Mbps	100 Mbps	300 Mbps	1 Gbps	5 Gbps	8 Gbps
VPN-tunneleita	10	500	5000	20 000	40 000	40 000
Samanaikaisia yhteyksiä	4 000	300 000	1 milj.	10 milj.	10 milj.	10 milj.
Klusterointi	ei	kyllä	kyllä	kyllä	kyllä	kyllä

Virtuaalinen palomuuri toimii käytännössä samalla tavalla kuin valmiit laitteet, molempia hallitaan SMC:n kautta ja niissä ajetaan samoja versioita palomuuriohjelmistosta. Se toimitetaan valmiina virtuaalikoneena, joka voidaan tuoda suoraan virtualisointialustaan ja ottaa nopeasti käyttöön. Stonesoft on kehittänyt palomuureja virtuaalialustoille vuodesta 2002 lähtien. StoneGate-virtuaalipalomuuri on virallisesti sertifioitu VMware ESX Server -alustalle mutta sitä pystyy ajamaan myös muiden valmistajien samantyyppisillä virtualisointialustoilla (24). Käytännössä täysi toimivuus taataan ja tuotetta tuetaan kuitenkin vain seuraavilla VMwaren alustoilla mainituissa ja uudemmissa versioissa: VMware ESX Server 3.5.0, VMware vSphere Hypervisor ESXi 4.1, VMware Workstation 6.0 ja VMware Player. (25.)

Virtuaalista palomuuria ei voi suoraan verrata mihinkään StoneGate-laitteeseen, koska sen suorituskyky riippuu hyvin pitkälle siitä, kuinka paljon resursseja sille allokoidaan. Virtuaalisen palomuurin vähimmäisvaatimukset ovat 2 GB kiintolevytilaa ja 256 MB RAM-muistia, tosin suositellut arvot ovat 8 GB edelliselle ja 1 GB jälkimmäiselle (25). Vertailun vuoksi esimerkiksi valikoiman alkupään StoneGate FW-310 -palomuurissa on 1 GB RAM-muistia. Kapasiteetti voi helposti jäädä liian pieneksi, jos palomuurin virtuaalikoneelle on allokoitu liian vähän muistia, vähimmäismäärä 256 MB RAM-muistia mahdollistaisi esimerkiksi reilusti alle tuhat samanaikaista yhteyttä palomuurin läpi. Toisena vertailukohtana 2 GB:n RAM-muistin avulla palomuuri pystyisi hoitamaan jo pari tuhatta VPN-tunnelia. Stonesoft ei ole määritellyt prosessorille vähimmäisvaatimuksia, koska vaikka useimmissa virtuaalialustoissa virtuaalikoneen prosessoritehoa voidaan rajoittaa, siihen ei usein ole tarvetta. Virtuaalikoneelle voi tosin määrittää useamman prosessorin, jos sen on tarkoitus käsitellä suuria liikennemääriä. Lukuun ottamatta VPN-liikenteen vaatimaa suurempaa prosessoritehoa RAM-muisti on yleisimmin palomuurin pullonkaula, varsinkin jos sillä tehdään paljon IPS-tyylistä liikenteen sovellustason tutkintaa.

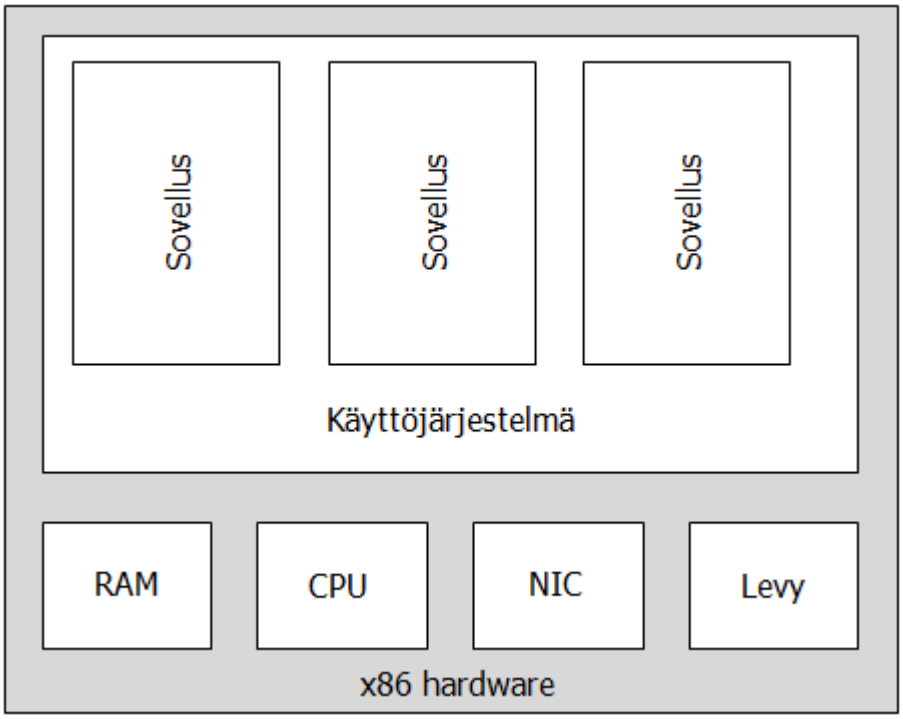
4 Virtualisointi

4.1 Virtualisoinnin perusteita

Virtualisointi itsessään on melko laaja käsite, jolla viitataan resurssien abstraktointiin, jossa esimerkiksi yksi fyysinen resurssi voi toimia monena loogisena resurssina. Yleisesti käytettyjä virtualisointitekniikoita ovat muun muassa käyttöjärjestelmätason, laiteresurssien, laitteiston ja ohjelmiston virtualisointi. Käyttöjärjestelmätason virtualisointi on vanhempi tekniikka, jota käytetään suurissa mainframe-koneissa, kuten IBM:n eServer zSeriesissä, usean erillisen käyttöjärjestelmäympäristön ajamiseen samanaikaisesti. VMware-alustoille kehitetyn virtuaalipalomuurin lisäksi Stonesoft on myös julkaissut samanlaisen tuotteen vuonna 2003 juuri IBM eServer zSeries -koneille (21).

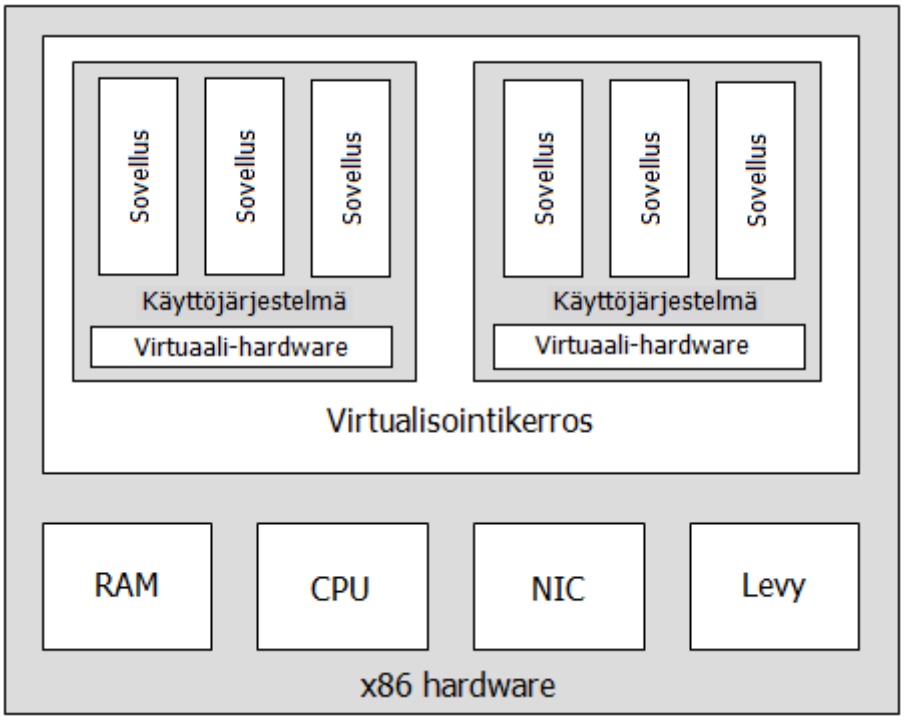
Laiteresurssien virtualisointi on yksi yleisimmin käytetyistä tekniikoista, jonka avulla voidaan esimerkiksi muodostaa useammasta kiintolevystä yksi suurempi looginen levy tai virtualisoida RAM-muistia sivuttamalla sitä kiintolevylle. Prosessorien virtualisointitekniikat ovat tällä hetkellä yleisimpiä laitteistovirtualisoinnin esimerkkejä. Nykyprosessoreissa on erilaisia turvatasoja, jotka määrittävät niillä ajettavien prosessien oikeudet. Esimerkiksi virtuaalikoneita ajetaan yleensä vähiten luotetulla tasolla, jolloin ne eivät pysty tekemään suoraan kernelikutsuja prosessorille. Virtualisoimalla prosessorin turvatasoja myös virtuaalikoneiden käyttöjärjestelmille voidaan antaa laajemmat oikeudet kerneliin ilman sen muokkausta. Yksi ohjelmistovirtualisoinnin tyypeistä on esimerkiksi Javan käyttämä virtuaalikone Java Virtual Machine, jossa ajetaan Java-tavukoodia käyttöjärjestelmästä loogisesti erillisessä ympäristössä. Tällä ratkaisulla samaa koodia voidaan ajaa millä tahansa alustalla ja saavutetaan parempi tietoturva, koska komennot ajetaan käyttöjärjestelmästä loogisesti eriytetyssä ympäristössä. Toinen ohjelmistovirtualisoinnin tyyppi, jota tästä eteenpäin käsitellään pääasiassa, on kokonaisten tietokoneiden virtualisointi ohjelmiston avulla. Ohjelmallisen virtualisointikerroksen avulla fyysisessä koneessa voidaan ajaa useaa toisistaan täysin erillistä virtuaalikonetta, joissa ajetaan omaa käyttöjärjestelmää ja jotka käyttäytyvät samalla tavalla kuin oikea tietokone. (28, s. 19.)

Yleisimmin yrityskäytössä virtualisoidaan erilaisia palvelimia mutta jotkin yritykset ovat tuoneet markkinoille myös muita virtuaalisia laitteita. Cisco julkaisi vuonna 2008 ensimmäisen virtuaalikytkimensä Nexus 1000V:n, joka on suunniteltu VMwaren ESX-palvelimille. Erinäiset tietoturvayritykset ovat julkaisseet myös virtuaalisia tietoturvalaitteita, kuten palomuureja ja IPS:iä, mutta tarjolla on myös ilmaisia avoimen lähdekoodin ohjelmistoja. Virtualisointiratkaisujen valmistajista suurimpia ovat tällä hetkellä VMware ESX ja ESXi-ratkaisuillaan, Citrix XenServer-ratkaisullaan ja Microsoft Hyper-V Server -ratkaisullaan.



Kuvio 8. Tavallisen x86-tietokoneen pelkistetty arkkitehtuuri.

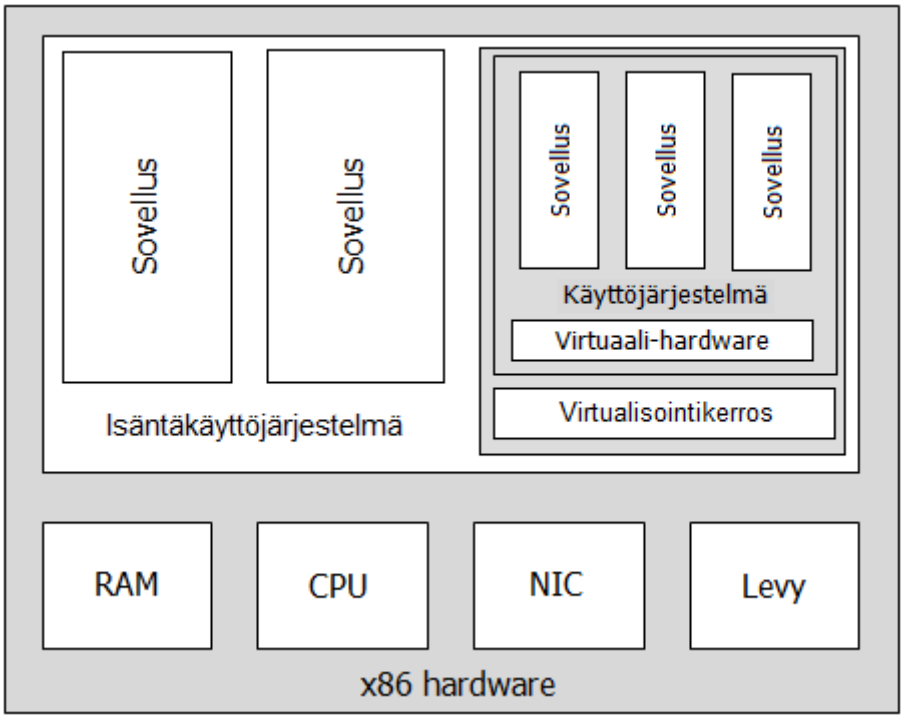
Kuviossa 8 on esitetty, miten tavallinen tietokone tarjoaa laitteiston eli muun muassa keskusmuistin, prosessorin, verkkosovittimet ja kiintolevyn käyttöjärjestelmän käyttöön. Kuvio 9 taas esittää, kuinka virtualisoinnin avulla tietokoneen fyysiset resurssit jaetaan useampaan virtuaaliseen segmenttiin tai toisin sanoen virtuaalikoneeseen. Virtuaalikoneiden käyttöjärjestelmä erotetaan laitteistosta virtualisointikerroksen avulla, joka hoitaa fyysisten resurssien jakamisen. (26, s. 2.)



Kuvio 9. Esitys virtuaalikoneista x86 hypervisor -arkkitehtuurissa.

Virtualisointiterminologiassa isäntäkone (engl. host machine) on itse fyysinen kone ja isäntäkäyttöjärjestelmä kyseiseen koneeseen asennettu käyttöjärjestelmä. Virtuaalikone on fyysisellä tietokoneella oleva eristetty osio. Kun virtuaalikone ensin luodaan, se on tyhjä. Virtuaalikoneeseen asennettavaan käyttöjärjestelmään viitataan termillä vieraskäyttöjärjestelmä (engl. guest operating system). Virtualisointikerros voidaan pääasiassa toteuttaa kahdella eri tavalla eli hosted- tai hypervisor-arkkitehtuurina. Hosted-arkkitehtuurissa virtualisointiohjelmisto on asennettu olemassaolevaan isäntäkäyttöjärjestelmään, käsitettä on visualisoitu kuviossa 10. Virtualisointikerros on siis riippuvainen isäntäkäyttöjärjestelmän kyvystä tukea kaikkia käytettyjä fyysisiä laitteita. Tämä mahdollistaa toisaalta sen, että virtuaalikerroksella on käytettävissä paljon suurempi laitteiden kirjo, koska yleisimmät käyttöjärjestelmät tukevat miltei kaikkia laitteita. Ratkaisu on helppo ottaa käyttöön mutta huonona puolena on se, että isäntäkäyttöjärjestelmäkin kuormittaa laitteistoa omalta osaltaan ja ylläpitäjien on pidettävä huolta myös muun muassa sen käyttöoikeuksista ja päivittämisestä. VirtualBox, VMware Server ja VMware Workstation ovat hyviä esimerkkejä tämän tyyppisestä virtualisoinnista. (26, s. 3—6.)

Hypervisor-arkkitehtuurissa, jota kuvio 9 myös esittää, virtualisointiohjelmisto on asennettu suoraan palvelimelle eli itse tietokoneessa ei tarvitse olla olemassaolevaa käyttöjärjestelmää vaan virtualisointiohjelmisto asentaa oman kernelinsä ja laiteajurinsa. Tavallisen käyttöjärjestelmän sijasta virtualisointiohjelmiston on siis tarjottava kerneli- ja ohjaintukea fyysisille resursseille. Tämä ratkaisu eliminoi käyttöjärjestelmän niin sanotun kiinteän kuormituksen mutta toisaalta vähentää merkittävästi vaihtoehtoja käytettävän raudan suhteen. Tämä johtuu siitä, että virtualisointiratkaisun toimittajan, kuten VMwaren, on kirjoitettava laiteajurit itse, joten se joutuu valitsemaan rajatun määrän tuettuja laitteita. VMware ESX ja sen ilmaisversio ESXi ovat hyviä esimerkkejä hypervisor-arkkitehtuuria käyttävistä tuotteista. (26, s. 3—5.)



Kuvio 10. Hosted-arkkitehtuurina toteutettu virtualisointi

Virtualisoinnilla on useita etuja, joiden takia se on yleistynyt hyvin nopeasti. Yksi ilmiselvä hyöty on usean erilaisen käyttöjärjestelmän, kuten Windowsin ja Linuxin, ajaminen samanaikaisesti samalla tietokoneella. Uusien virtuaalikoneiden nopea käyttöönotto on mahdollista käyttämällä valmiiksi luotuja levykuvia. Voidaan esimerkiksi luoda levykuva CentOS Linux –koneesta, johon on valmiiksi asennettu ja konfiguroitu HTTP-palvelin, joka voidaan ottaa käyttöön tarvittaessa muutamassa

minuutissa tuomalla levykuva virtualisointiohjelmistoon. Kun vaihtoehto on fyysisen palvelimen hankkiminen ja käyttöjärjestelmän asentaminen ja konfiguroiminen, voidaan helposti nähdä, miten virtualisointi helpottaa esimerkiksi palvelinylläpitäjien elämää. Koska virtuaalikone on käytännössä vain pari tiedostoa kovalevyllä, sen varmuuskopiointi on hyvin helppoa. Mahdollisuus siirtää ja kopioida virtuaalikoneita tuo lisää tietoturvaa, koska esimerkiksi viallinen virtuaalikone on hyvin helppo korvata siirtämällä varmuuskopio toiseen palvelimeen. Perinteisen varmuuskopioinnin lisäksi virtuaalikoneesta voi ottaa niin sanotun tilannevedoksen (engl. snapshot) esimerkiksi ennen suurta ohjelmistopäivitystä. Jos päivitys menee pieleen, päästään päivitystä edeltävään vakaaseen tilaan nopeasti palauttamalla kyseinen tilannevedos. Yksi helpoiten myytäviä argumentteja virtualisoinnin hyväksi on, että se vähentää kuluja käyttämällä laitteistoa tehokkaammin hyväkseen. On arvioitu, että palvelimien päivittäinen käyttöaste on globaalisti vain noin 5—10 % (27). Jos verrataan kahta palvelinta, joilla on sama ostohinta mutta toisella kaksi kertaa korkeampi käyttöaste, on helppo nähdä, kumpi vaihtoehto on taloudellisempi. Yhdistämällä olemassaolevia fyysisiä palvelimia virtuaalialustalle voidaan helposti nostaa palvelimien käyttöastetta ja pääoman tuottoastetta.

4.2 VMware-virtualisointiratkaisut

Työssä käsitellään VMwaren tuotteista vain Workstationia, Serveriä, ESX:ää ja ESXi:tä, koska testattava StoneGate-virtuaalipalomuuri on pääasiassa tarkoitettu käytettäväksi vain niillä. VMware Workstation on vuonna 1999 julkaistu olemassaolevaan käyttöjärjestelmään asennettava virtualisointiohjelmisto. Workstation soveltuu pääasiassa vain paikalliseen käyttöön, koska virtuaalikoneita voi ajaa vain silloin kun käyttäjä on kirjautuneena isäntäkoneelle. Workstation ei myöskään tarjoa ollenkaan etäkäyttömahdollisuutta, eli virtuaaliympäristöä voi hallita vain kyseiseltä isäntäkoneelta. Näistä syistä johtuen VMware Workstationia ei juurikaan näe tuotantokäytössä vaan muun muassa kehittäjät käyttävät sitä testaukseen, kuten tämänkin työn yhteydessä tehdään. VMware Server on vuonna 2006 julkaistu seuraaja lakkautetulle GSX Server –tuotteelle, ja kuten Workstation sekin käyttää hosted-arkkitehtuuria. VMware Serverin virtuaaliympäristöä voi hallita etänä, ja se tarjoaa myös pääsyä virtuaalikoneiden konsoleille etänä. Serverin suurin rajoitus on, että se joutuu käyttämään tietokoneen fyysisiä resursseja isäntäkäyttöjärjestelmän kautta,

joka rajoittaa tuotteen skaalautuvuutta ja suoritustehoa. Syy rajoituksiin on teknisesti se, että virtuaalikoneet eivät voi käyttää fyysisiä resursseja suoraan. Esimerkkinä jos virtuaalikoneelle määritetään tietty määrä muistia, se ei saa sitä suoraan käyttöönsä, sen sijaan aina kun virtuaalikoneen tarvitsee käyttää muistia se joutuu pyytämään sitä isäntäkäyttöjärjestelmältä. Jos isäntäkone on kuormitettu, on mahdollista, että muut prosessit ajavat virtuaalikoneen pyynnön edelle, jolloin sen suorituskyky laskee. (28, s. 25.)

VMware ESX ja ESXi ovat hypervisor-tyyppisiä virtualisointiratkaisuja, ESX julkaistiin vuonna 2001, ja ESXi lohkaistiin ESX:stä omaksi ilmaistuotteekseen vuonna 2007. Molempien tuotteiden vahvuuksia ovat suorituskyky, hallintaominaisuudet ja luotettavuus. Suorituskyky on hosted-tyyppisiin tuotteisiin verrattuna aivan eri tasolla, koska hypervisor-arkkitehtuuri on kokonaista käyttöjärjestelmää paljon kevyempi ja pystyy hyödyntämään fyysisiä resursseja virtuaalikoneiden hyväksi tehokkaammin. Resursseja voi myös jakaa tarkemmin ja virtuaalikoneiden suorituskykyä hienosäätää pidemmälle. vMotion-teknologia mahdollistaa virtuaalikoneiden siirtämisen helposti palvelimelta toiselle ilman palvelukatkoksia, ja se voi myös automaattisesti tasata kuormaa ESX-klusterin toisille jäsenille siirtämällä virtuaalikoneita palvelimien välillä. VMware High Availability -teknologia puolestaan tarjoaa vikasietoisuutta, ESX-palvelimen hajotessa virtuaalikoneet käynnistetään välittömästi uudelleen toisella palvelimella muutamassa minuutissa. Ratkaisujen luotettavuutta nostaa VMwaren ylläpitämä lista ESX:n ja ESXi:n kanssa yhteensopivista testatuista laitteista. (28, s. 26—27.)

VMware ESX koostuu kahdesta komponentista eli kernelistä (VMkernel) ja Service Consolesta. Service Console on kustomoitu Linux-kerneli eli periaatteessa vain virtuaalikone, jonka avulla voi hallita VMkernelin konfiguraatiota. VMkernel on palvelimen sydän, joka on rakennettu alusta alkaen pelkästään jakamaan ja hallinnoimaan fyysisiä resursseja. Tämä tekee siitä hyvin kevyen mutta tehokkaan. Toisin kuin tavalliset käyttöjärjestelmät, kuten Windows ja Linux, joiden kuormitus voi olla helposti 10—20 %, VMkernel kuormittaa järjestelmää vain noin 3—8 %. VMkernelin päätehtävä on siis hallita virtuaalikoneiden käyttämää muistia, prosessoriaikaa, virtuaalikytkimiä ja pääsyä muistivarastoihin, eli se toimii virtualisointikerroksena. VMware ESXi eroaa ESX:stä siten, että siinä on eliminoitu

Service Console kokonaan, minkä ansiosta ESXi kuormittaa konetta vielä vähemmän. ESXi:n ilmaisversiosta pois jätettyjä ominaisuuksia voi myös hyödyntää maksamalla niistä erikseen. ESX:n ominaisuuksia, kuten vMotionia ja High Availabilityä, voi hyödyntää ostamalla niille erilliset lisenssit. VMware on alkanutkin viimeisimpien julkaisujensa yhteydessä patistamaan ihmisiä siirtymään ESX:stä sitä kehittyneempään ESXi:hin. Tästä esimerkkinä uusin vSphere 5, joka tukee pelkästään ESXi:tä. (28, s. 28.)

4.3 Virtuaaliset tietoverkot

Virtuaalisilla tietoverkoilla viitataan tässä virtuaaliympäristössä, kuten VMware ESX:ssä tai Workstationissa, sijaitseviin tietoverkkoihin ja niiden sisäiseen tietoliikenteeseen. Verkkojen virtualisointi ei ole sinällään uusi käsite, sillä sitä on tehty tavallisissa fyysisissä tietoverkoissakin jo vuosia. Tavallisessa verkossa tietoliikennettä, verkkoja ja käyttäjiä voidaan jakaa mielivaltaisesti erilaisiin osiin ohjelmiston virtualisoinnilla muun muassa kytkimissä ja reitittimissä. Perinteisessä kytkentäisessä verkossa kaikki yhdessä kytkimessä kiinni olevat laitteet olivat aina samassa aliverkossa ja näin ollen myös samassa Layer 2 -verkkoalueessa. Yksi kytkin voidaan nykyään jakaa useaan L2-verkkoalueeseen ja aliverkkoon VLAN- eli Virtual Local Area Network –tekniikalla. Yhdestä fyysisestä kytkimestä voidaan virtualisointitekniikoilla siis luoda useampi looginen kytkin. Reitittimien reititystauluja myös virtualisoidaan esimerkiksi operaattorikäytössä muun muassa tietoturvasyistä, etteivät eri asiakkaat pääse toistensa verkkoihin. Ilman virtualisointia samat rajoitukset pitäisi toteuttaa esimerkiksi pääsylistoilla, joiden ylläpito olisi hyvin aikaavievää. Toinen syy reititystaulujen eriyttämiseen on se, että eri asiakkailla voi olla käytössä päällekkäisiä yksityisiä verkkoja, jolloin kaikkia ei edes voisi pitää yhteisessä reititystaulussa.

VMware Workstation tarjoaa useita eri tapoja yhdistää virtuaalikone verkkoon. Jokaiselle virtuaalikoneelle pitää ensinnäkin määrittää yksi tai useampi virtuaalinen verkkosovitin verkkoyhteyksiä varten. Yhdellä virtuaalikoneella voi olla Workstation 6.0 -versiosta ylöspäin korkeintaan kymmenen verkkosovitinta. Virtuaalikytkimet, eli VMwaren terminologiassa vSwitchit, ovat Layer 2 -tasolla toimivia kytkimiä. Valmiit virtuaalikytkimet identifioidaan Workstationissa nimillä VMnet0—VMnet9, eli niitä on käytettävissä kymmenen, tosin dokumentaation mukaan Workstationin pitäisi luoda

tarvittaessa lisää kytkimiä automaattisesti. Yhteydet virtuaaliympäristöstä ulkomaailmaan menevät luonnollisesti isäntäkoneen verkkosovittimen läpi. Virtuaalikoneen voi yhdistää ulkoverkkoon joko VMnet0:n avulla, joka siltaa virtuaalisen verkkosovittimen isäntäkoneen verkkosovittimeen tai VMnet8:n avulla, joka NAT:a käyttämällä muuntaa ulospäin menevän liikenteen lähdeosoitteen isäntäkoneen verkkosovittimen IP-osoitteeksi. Kun virtuaalisovitin sillataan fyysiseen verkkosovittimeen, sille pitää määrittää IP-osoite joko käsin tai ulkoverkossa olevan DHCP-palvelimen avulla. Sillattua verkkoyhteyttä käyttävä virtuaalikone näkyy ulkoverkon laitteille samalla tavalla kuin mikä tahansa fyysinen laite, esimerkiksi ulkoisen kytkimen näkökulmasta isäntäkoneen verkkosovittimella on kaksi IP-osoitetta. Yhdistettäessä virtuaalikone ulkoverkkoon VMnet8:n eli NAT:n avulla, Workstation voi antaa sille IP-osoitteen oman DHCP-palvelimensa avulla. Käytettäessä VMnet8:aa virtuaalikone ja isäntäkone näkyvät ulkoverkkoon yhtenä laitteena. NAT-konfiguraatio hidastaa verkkoyhteyksiä hieman ylimääräisen pakettien käsittelyn takia eikä NAT:n takana oleviin virtuaalikoneisiin saa yhtä helposti yhteyttä ulkoverkosta ilman erillistä konfiguraatiota. (29.)

VMnet1, jota kutsutaan ”host-only networking”-verkoksi, mahdollistaa virtuaalikoneiden ja isäntäkoneen välisen kommunikaation tilanteissa, joissa virtuaalikoneilla ei tarvitse olla yhteyttä ulkoverkkoon. Isäntäkoneelle luodaan automaattisesti virtuaalinen verkkosovitin, joka on yhteydessä VMnet1:een, mahdollistaen kommunikoinnin siihen kytkettyjen virtuaalikoneiden kanssa. Kaikki VMnet1:een yhdistetyt virtuaalikoneet voivat myös kommunikoida keskenään mutta muuten kyseinen verkko on eristetty täysin ulkomaailmasta, ellei liikennettä erikseen reititetä VMnet1:stä fyysiseen verkkosovittimeen. Reititys voidaan tehdä joko isäntäkoneessa tai erillisen virtuaalikoneen avulla. (29.)

Virtuaalikytkimillä voi luoda melko monimutkaisenkin verkon, koska Workstationin kymmenen kytkimen rajoituksen sijaan ESX tukee 127:ää kytkintä. Jokaiselle virtuaalikytkimelle voi määritellä oman verkkonsa, ja virtuaalikytkin voi myös jakaa tästä verkosta virtuaalikoneille osoitteita virtuaalisen DHCP-palvelimensa avulla. Tietoverkkojen osalta VMware Workstationin ja ESX:n ero on se, että jälkimmäisessä verkko konfiguroidaan pelkästään virtuaalikytkimien avulla. Yhteydet ulkoverkkoon menevät ESX:ssä virtuaalikytkimien kautta, joihin voidaan liittää yksi tai useampi

fyysinen verkkosovitin. Kun virtuaalikytkimeen liitetään kaksi tai useampi verkkosovitin kytkimen kautta ulkoverkkoon menevää liikennettä voidaan joko jakaa tasaisesti jokaiselle fyysiselle verkkosovittimelle tai yhtä tai useampaa verkkosovitinta voidaan pitää varalla valmiustilassa. Yleisin konfiguraatio on asentaa isäntäkoneeseen 2—5 verkkosovitinta vikasietoisuuden ja korkeamman verkon suoritustehon vuoksi. Ainakin yksi verkkosovitin on syytä omistaa hallintayhteyksille ja kommunikaatiolle muiden ESX-palvelimien kanssa. Isäntäkoneiden on tarpeen kommunikoida keskenään esimerkiksi vMotion ja HA-ominaisuuksien takia, kun virtuaalikoneita pitää siirtää isäntäkoneelta toiselle. Loput verkkosovittimet voidaan näin antaa pelkästään virtuaalikoneiden käyttöön.

ESX mahdollistaa myös VLAN:ien käytön, joilla voidaan loogisesti segmentoida verkkoa ilman uusien virtuaalikytkimien luontia. IEEE:n standardissa 802.1q määritelty VLAN-tekniikka vaatii, että paketteihin liitetään 32-bittinen VLAN-kenttä eli tagi. Tarkastelemalla tätä VLAN-tagia L2-verkkolaitteet kuten kytkimet voivat päätellä, miten paketti pitäisi välittää eteenpäin. ESX voi hyödyntää VLAN:eja pääasiassa kahdella eri tavalla, eli tieto VLAN:sta voidaan merkitä pakettiin joko isäntäkoneen ulkopuolella tai sisäpuolella. Ulkoinen kytkin, johon isäntäkoneen fyysiset verkkosovittimet on kytketty, voi lisätä VLAN-tagin isäntäkoneelle meneviin paketteihin. Kytkimessä on määriteltävä, mihin VLAN:iin jokainen isäntäkoneelle johtava portti kuuluu, ja ESX:ssä jokaiselle VLAN:lle on luotava oma virtuaalikytkimensä. Tämä on yksinkertaisin konfiguraatio mutta näin VLAN:eja ei voi olla käytössä enempää, kuin isäntäkoneessa on verkkosovittimia. Käsiteltäessä VLAN:eja sisäisesti ulkoisen kytkimen ESX:ään johtavat portit on määriteltävä niin sanotuiksi trunk-porteiksi, joiden läpi kulkee useamman kuin yhden VLAN:n liikennettä. Sisääntulevien pakettien tagaus tapahtuu kuten normaalistikin ulkoverkon kytkimissä. ESX:n fyysiset verkkosovittimet taas hoitavat VLAN-tagien lisäyksen isäntäkoneesta ulospäin meneviin paketteihin, jolloin pakettien muokkaus ei rasita VMkerneliä. Tämäntyyppisessä konfiguraatiossa on suositeltavaa määrittää ESX:ään vain yksi virtuaalikytkin, joka yhdistetään kaikkiin fyysisiin verkkosovittimiin. Jotta tämä virtuaalikytkin pystyisi välittämään paketteja oikein, sen pitää tietää, mikä siihen yhdistetty virtuaalisovitin kuuluu mihinkin VLAN:iin. Tämä on mahdollista määrittelemällä virtuaalikytkimelle jokaiselle VLAN:lle oma porttiryhmä (engl. port group). Yhdistettäessä virtuaalikoneen verkkosovitin tähän

virtuaalikytkimeen VLAN määritellään liittämällä sovitin oikeaan porttiryhmään. (28, s. 202—205.)

Virtuaalisten tietoverkkojen suunnittelussa on otettava huomioon samat rajoitukset kuin fyysisessä verkossa. Virtuaalikytkimet käsittelevät tietoliikennettä vain L2-tasolla, eli jos eri aliverkoissa olevien virtuaalikoneiden on tarkoitus kommunikoida keskenään, tarvitaan väliin jokin reititystä tekevä L3-tason laite. Tämä voi olla yksinkertaisimmillaan tavallinen Linux-virtuaalikone, joka on yhdistetty kahteen tai useampaan virtuaalikytkimeen eli aliverkkoon ja konfiguroitu reitittämään paketteja. Toinen ratkaisu on käyttää tarkoitukseen siihen suunniteltua virtuaalista tietoturva- tai verkkolaitetta. Ciscon virtuaalisen monitasokytkimen Nexus 1000V:n lisäksi on olemassa myös avoimen lähdekoodin ratkaisuja, kuten Untangle ja Vyatta. Useimmat virtuaalipalomuurit, kuten StoneGate, pystyvät myös tekemään reititystä. StoneGaten tavoin Untangle ja Vyatta pystyvät reitityksen lisäksi toimimaan myös palomuureina ja VPN-yhdyskäytävinä.

Tietoliikennettä virtuaaliympäristön sisällä virtuaalikoneesta toiseen käsitellään hieman eri tavalla kuin perinteisessä fyysisessä verkossa, koska se pysyy täysin isäntäkoneen sisällä. Virtuaalikytkimet tukevat VMware ESX 3 -versiosta lähtien 1016:ta virtuaalista verkkosovitinta. Kahden samassa virtuaalikytkimessä kiinni olevan virtuaalikoneen kommunikoidessa toistensa kanssa kaikki liikenne menee pelkästään isäntäkoneen sisäisen laiteväylän yli kuormittamatta fyysistä verkkoa ollenkaan. Tiedonsiirto on näin ollen yleensä vähintään yhtä nopeaa kuin fyysisessä lähiverkossa, koska VMkernel vain siirtää välitettävän datan muistissa virtuaalikoneelta toiselle. Isäntäkoneen prosessori käsittelee kaiken virtuaalikoneiden välisen tiedonsiirron, joten prosessoria ei kannata ylikuormittaa aivan äärirajoille, ettei virtuaalikoneiden välinen tietoliikenne kärsi. Prosessorin lisäksi virtuaalikoneiden välisen liikenteen maksiminopeus määräytyy pääasiassa koneiden TCP/IP-pinojen mukaan; prosessorin ylikuormittuessa TCP ottaa käyttöön ruuhkanhallintamekanismeja, jotka hidastavat tiedonsiirtoa entisestään. Samassa virtuaalikytkimessä kiinni olevien keskenään kommunikoivien virtuaalikoneiden pitää olla myös samassa VLAN:ssa, muutoin pakettien on mentävä jonkin reitittävän laitteen läpi. Virtuaalikoneiden välisen liikenteen toimintaperiaatteet on hyvä pitää mielessä suunnitellessa verkkoa varsinkin, jos virtuaalikoneissa ajetaan korkeaa tietoturvaa tai liikenteen valvontaa vaativia palveluita. Koska virtuaalikoneiden

välinen liikenne kulkee pelkästään isäntäkoneen sisällä, sitä ei voi nähdä tai tutkia perinteisten fyysisten tietoturvalaitteiden kuten palomuurien ja IPS:ien avulla. (28, s. 190.)

4.4 Virtuaaliympäristön tietoturva

Viimeaikaisten tutkimusten mukaan 60 % virtualisoiduista palvelimista on tietoturvaltaan huonompia kuin fyysiset palvelimet (30). Yritysten ottaessa käyttöön sekä markkinoille että itselleen verrattain uusia virtualisointiteknologioita tietoturva jää usein taka-alalle virtualisoinnin helppouden ja tavoiteltujen kustannussäästöjen takia. Perinteisen tietoturvan integrointi virtuaaliympäristöön voi myös syödä virtualisoinnilla saavutettuja kustannussäästöjä. Virtualisoidut tietoturvalaitteet ja virtuaalikoneiden tietoturvaohjelmistot luonnollisesti kuluttavat jonkin verran resursseja, mikä voi rajoittaa palvelimilla ajettavien virtuaalikoneiden määrää.

Virtuaaliympäristön tietoturva voidaan jakaa karkeasti kolmeen alueeseen: virtuaalikoneiden, isäntäkoneen ja virtuaalisen tietoverkon tietoturva. Saman tietoturvapolitiikan, joka koskee fyysisiä tietokoneita, pitäisi myös koskea virtuaalikoneita, olivat ne sitten palvelimia tai työpöytiä. Virtuaalikoneiden prosessorikutsut ja muistialueet on tehokkaasti eriytetty toisistaan, joten niitä koskevat pääasiassa vain samat tietoturvauhat kuin fyysisiä koneita. Vieraskäyttöjärjestelmiä ja ohjelmistoja on ensinnäkin syytä päivittää aktiivisesti. Tämä on erityisen tärkeää, koska päivitykset on helppo unohtaa, kun uusia virtuaalikoneita voi luoda helposti parissa minuutissa. Virustorjunta on myös syytä pitää päällä ja ajan tasalla, koska virtuaalikoneita voi saastuttaa samalla tavalla kuin fyysisiä koneitakin. Usean virtuaalikoneen samanaikainen virustarkistus voi toisaalta kuluttaa leijonanosan isäntäkoneen resursseista, joten virtuaalikoneiden virustarkistuksia ei kannata ajastaa kaikkia alkamaan samaan aikaan. (28, s. 288—289.)

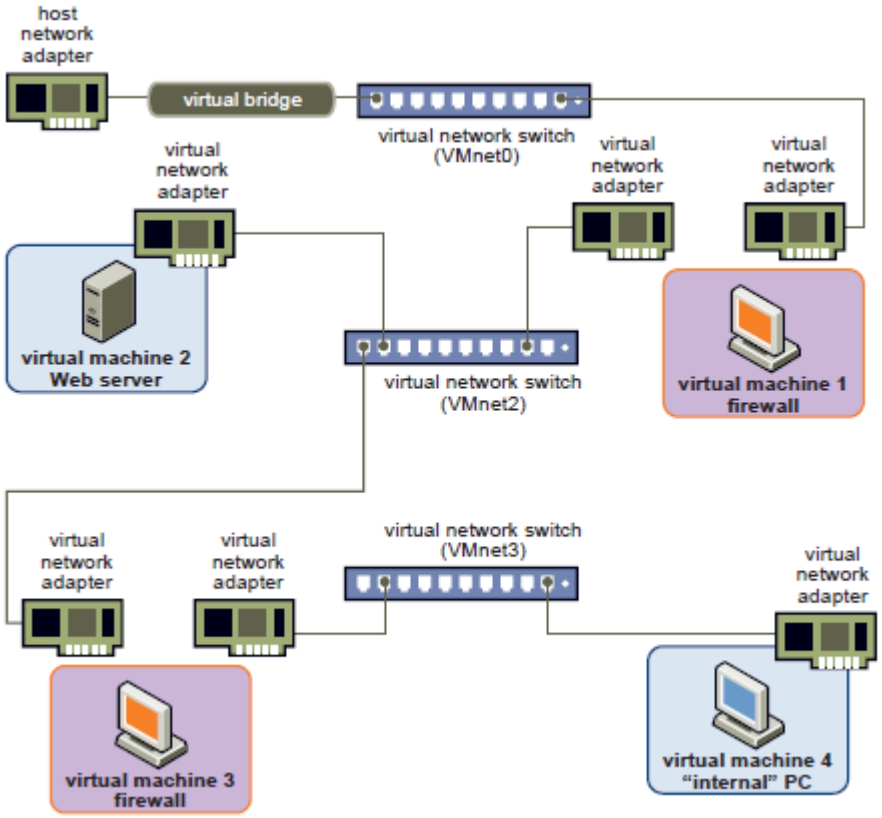
Isäntäkoneen suurimmat potentiaaliset tietoturvauhat koskevat käyttöoikeuksia ja pääsyä koneelle verkon välityksellä. Isäntäkoneen ohjelmisto on myös syytä pitää ajan tasalla ja VMware onneksi julkaiseekin korjauksia uusiin haavoittuvuuksiin melko nopeasti. ESX:ssä on otettava huomioon käyttöoikeudet Service Consoleen ja VirtualCenteriin, ESXi:ssä vain jälkimmäiseen. Käyttäjienhallinta on isommissa virtuaaliympäristöissä mahdollista keskittää myös ulkoiseen olemassaolevaan

hakemistopalveluun, kuten Active Directoryyn. Yhden isäntäkoneen käyttäjiä ja oikeuksia on vielä melko yksinkertaista hallita suoraan ESX:ssä mutta hallittaessa useampaa isäntäkonetta käyttäjienhallinta on helpompaa keskittää muualle. VirtualCenter asennetaan Windows-palvelimelle, joten siinä voidaan käyttää joko paikallista tai Active Directoryn käyttäjä- ja ryhmähakemistoa oikeuksien hallintaan. Käyttäjille voidaan määrittää erilaisia oikeuksia virtuaaliympäristön hallintaan, ja oikeuksien hallinta on luonnollisesti tärkeää tietoturvan kannalta, ettei kuka tahansa pysty rikkomaan ympäristöä. Pääsy ylläpitotyökaluihin, kuten Service Consoleen ja VirtualCenteriin, on myös hyvä rajata vain esimerkiksi tiettyihin koneisiin tai verkkoihin. Nämä pääsyrajoitukset voidaan konfiguroida suoraan isäntäkoneessa, koska Linuxiin pohjautuva ESX sisältää iptables-palomuurin. ESX:n iptables-palomuurin säännöt ovat oletuksena hyvin rajoittavat mutta niitä voi säätää sekä VirtualCenterin että Service Consolen kautta. (28, s. 273—287.)

Suunniteltaessa virtuaalisen tietoverkon topologiaa tietoturvan kannalta voidaan päätyä moneen eri ratkaisuun riippuen siitä millainen ympäristö on kyseessä. Helpoin ja perinteisin ratkaisu on sijoittaa isäntäkoneen eteen palomuuri, jonka läpi kaikki liikenne isäntäkoneelta ulos ja sisään kulkee. Tällä ratkaisulla voidaan hyödyntää olemassaolevaa verkkoinfrastruktuuria, ja se sopiikin hyvin pieniin virtuaaliympäristöihin. Ulkoinen palomuuri tarkoittaa toisaalta myös sitä, että virtuaaliympäristön sisäistä liikennettä voidaan valvoa vain jos se kierrätetään palomuurin kautta. Suurempien liikennemäärien kierrätys lisää latenssia ja kuormittaa isäntäkoneen ulkoisia verkkoyhteyksiä turhaan. Onkin järkevämpää ottaa käyttöön virtuaalinen palomuuri, jos virtuaalikoneet kommunikoivat paljon keskenään ja kyseistä liikennettä on valvottava. Palomuurin virtualisointi on hyvä ratkaisu myös luotaessa virtuaaliympäristöön DMZ-alue.

Yksi mahdollisuus on asettaa isäntäkoneen eteen fyysinen palomuuri, joka yhdistetään suoraan virtuaaliseen DMZ-verkkoon, josta taas pääsee virtuaalisen palomuurin läpi virtuaaliseen sisäverkkoon. Kuviossa 11 esitetty toinen vaihtoehto on virtualisoida myös fyysinen palomuuri ja sijoittaa DMZ kahden virtuaalipalomuurin väliin. DMZ voidaan toteuttaa toki ilman virtuaalipalomuureja määrittelemällä sille oma verkkosovittimensa virtuaalikoneesta, tällöin DMZ:stä virtuaaliseen sisäverkkoon menevä liikenne on tosin kierrätettävä ulkoisen palomuurin kautta. Varmin ratkaisu arkaluontoisten

virtualisoitujen palvelimien suojaamiseen, jotka tarvitsevat korkeaa tietoturvaa, on sijoittaa ne omalle erilliselle isäntäkoneelleen (28, s. 296). Pääsyä arkaluonteisille palvelimille ja niiden isäntäkoneelle voidaan näin rajoittaa tehokkaasti ja helposti. Hallintaliikenne ja niin sanottu virtuaalikoneiden tuotantoliikenne on myös syytä eristää toisistaan esimerkiksi omiin VLAN:eihinsa tai fyysisiin verkkosovittimiinsa. vMotionin tuottama liikenne sen siirtäessä virtuaalikoneita isäntäkoneelta toiselle on salaamatonta, joten senkin tietoturvaan on kiinnitettävä huomiota eristämällä se tuotantoliikenteestä.



Kuvio 11. Palomuurien integrointi virtuaaliseen verkkoon (29).

Tietoturvatoiminnot, kuten palomuurin tai IPS:n, voi sisällyttää myös isäntäkoneen hypervisoriin, jolloin ne toimivat periaatteessa virtualisointikerroksella. Hypervisor-pohjaisten palomuurien mainostetaan olevan kymmenen kertaa nopeampia kuin virtuaalikoneissa sijaitsevien palomuurien. Tämä johtuu siitä, että liikenne prosessoidaan VMkernelissä eikä silloin kun se kulkee palomuurin virtuaalikoneen läpi. VMwaren vuonna 2008 julkaisema VMsafe-teknologia mahdollistaa tietoturvalaitteiden integroinnin hypervisoriin tällä tavalla. VMsafe tarjoaa käytännössä hypervisoriin

erilaisia ohjelmointirajapintoja, joiden avulla voidaan valvoa muun muassa RAM-muistin, prosessorin, tietoverkon ja kiintolevyn käyttöä. Itse rajapinnat tuotiin yleisön käyttöön VMware vSphere 4 -virtualisointialustan julkaisun myötä vuoden 2009 lopussa. VMware siis vain tarjoaa ohjelmointirajapinnat kumppaneilleen, jotka voivat tehdä niitä hyödyntäviä virtuaalilaitteita. VMsafe on näin helpottanut kumppaniensa kehitystyötä, koska aikaisemmin vastaavien tuotteiden toteutus vaati VMkernelin muokkausta. (31.)

VMsafe-rajapintoja hyödyntävä tietoturvaratkaisu voidaan toteuttaa joko suoraan hypervisorissa tai virtuaalikoneessa, VMware kutsuu tapoja nimillä fast-path ja slow-path. Fast-path-rajapintaa hyödyntävä ratkaisu lataa VMkerneliin oman ajurinsa, joka suorittaa koodia, kun taas slow-pathia käyttävä ratkaisu suorittaa koodinsa virtuaalikoneessa samalla tavalla kuin perinteiset virtuaaliset tietoturvalaitteet. Todellisuudessa suurin osa VMsafe-tietoturvaratkaisuista yhdistävät molempia tapoja, koska pelkän kerneliajurin käyttö tekee hallinnasta ja valvonnasta hyvin vaikeaa. Miten ratkaisu on toteutettu, riippuu täysin laitevalmistajasta mutta suurin hyöty saavutetaan luonnollisesti tekemällä kaikki liikenteen prosessointi hypervisorissa. Kuormituksen ja nopeuden kannalta edullisin ratkaisu on ladata esimerkiksi koko palomuuripolitiikka hypervisoriin ja toteuttaa vain hallintaominaisuudet, kuten konfigurointi ja lokien kokoaminen virtuaalikoneessa. Toisaalta, koska fast-path on vain minimaaliseen hypervisor-käyttöjärjestelmään ladattu kerneliajuri, se ei välttämättä pysty tarjoamaan kaikkia samoja palveluita ja toimintoja kuin tavallinen palomuuri. Hypervisoria ei haluta myöskään paisuttaa liian isoksi, joten sinne ajuria varten ladattavan ylimääräisen koodin ja datan määrää on rajattava. Näin ollen yksi vaihtoehto on käsitellä tietty liikenne hypervisorissa ja siirtää esimerkiksi virusskannausta ja web-suodatusta vaativa liikenne palomuurin virtuaalikoneen käsiteltäväksi. (33.)

Hypervisor-rajapintoja hyödyntävälle tietoturvalaitteelle on yleensä luotava oma virtuaalikoneensa. Yksi tämän seikan eduista on se, että kyseisen virtuaalikoneen voi periaatteessa sijoittaa mihin tahansa paikkaan virtuaalisessa verkossa. Tämä virtuaalikone on silti syytä turvata kunnolla, koska sillä on laaja pääsy hypervisoriin ja näin ollen kaikkien virtuaalikoneiden muisti-, levy- ja verkko-operaatioihin. Tavalliset virtuaalipalomuurit ovat liikennevirran keskellä olevia virtuaalikoneita, joten niitä käytettäessä verkon hallinta voi olla monimutkaista, koska virtuaalikoneita voidaan

luoda ja siirtää nopeasti. Ylläpitäjillä on oltava selkeä käsitys verkkotopologiasta, ettei virtuaalikoneita esimerkiksi vahingossa yhdistetä vääriin virtuaalikytkimiin, jolloin palomuurit eivät enää suojaisikaan niitä. VMsafe mahdollistaa pakettisuodattimien sijoittamisen loogisesti jokaisen virtuaalikytkimen ja virtuaalikoneen verkkosovittimen väliin, jolloin ei-halutut paketit pudotetaan ennen kuin ne pääsevät virtuaaliselle verkkosovittimelle asti (32). Tämä teknologia ratkaisee esimerkiksi perinteisten ja virtuaalipalomuurien kyvyttömyyden valvoa virtuaalikoneiden välistä liikennettä. Se myös helpottaa verkonhallintaa, koska palomuurin suhdetta muihin virtuaalikoneisiin eikä sen paikkaa verkkotopologiassa tarvitse miettiä, sillä yksi hypervisor-pohjainen palomuuri pystyy valvomaan kaikkea virtuaaliympäristön tietoliikennettä.

VMsafea hyödyntäviä tuotteita ei ole vielä saataville erityisen paljon, koska kyseessä on suhteellisen tuore teknologia. VMsafea hyödyntäviä palomuureja ovat muun muassa Reflex Systemsin vTrust, Check Pointin Security Gateway Virtual Edition ja Juniper Networksin vGW. Valitettavasti moni laitevalmistaja ei erittele markkinointimateriaaleissaan erityisen selkeästi, miten ne ovat toteuttaneet hypervisor-pohjaiset tuotteensa. Juniper vGW on näistä kolmesta ainoa palomuuri, jonka mainostetaan toimivan täysin hypervisor- eli fast-path-tasolla (34). Juniper osti Altor Networksin vuonna 2010, ja vGW pohjautuu Altorin aiemmin kehittämiin hypervisor-pohjaisiin palomuureihin. StoneGate toimii täysin slow-path-tasolla, eli sitä ei ole integroitu hypervisoriin millään tavalla vaikka VMsafe-tuki mainitaankin vielä virheellisesti tuotteen datalehdessä (36). Muista hypervisor-pohjaisista tietoturvatuotteista yksi esimerkki on Trend Micron Deep Security, joka voi IDS- ja palomuuritoimintojen lisäksi suojella virtuaalikoneita viruksilta ja haittaohjelmilta (35). Deep Security mahdollistaa muun muassa virusskannauksen keskittämisen yhteen virtuaalikoneeseen, jolloin skannauksia ei tarvitse erikseen aikatauluttaa alkamaan eri aikoihin. Ratkaisu myös eliminoi tarpeen asentaa ylimääräistä virustorjuntaohjelmistoa kaikkiin virtuaalikoneisiin, minkä ansiosta resursseja vapautuu muuhun käyttöön.

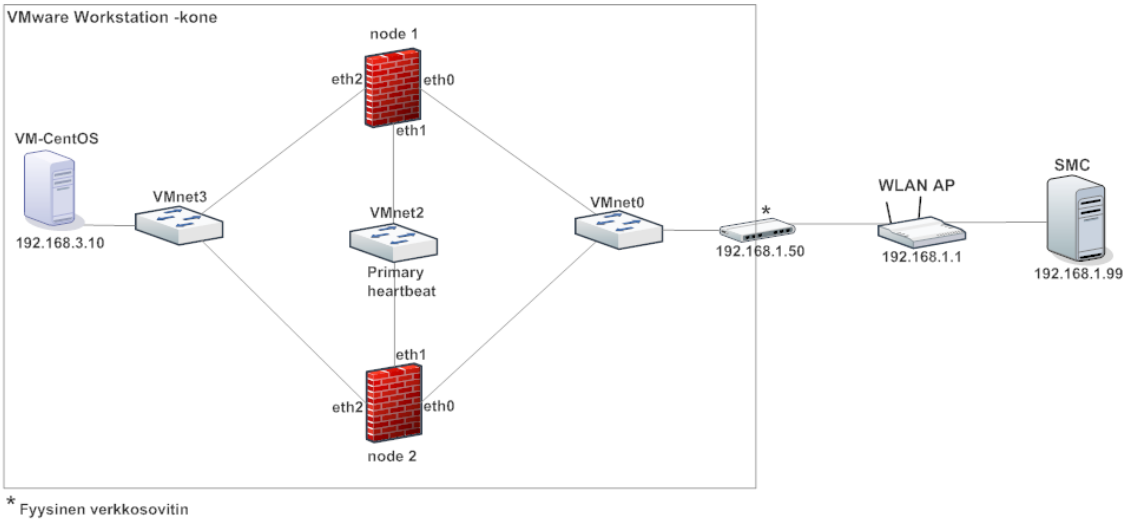
Hypervisor-pohjaisten palomuurien etuja virtuaalikonepohjaisiin palomuureihin ovat pääasiassa nopeampi liikenteen prosessointikyky ja selkeämpi hallittavuus. Hallittavuus on parempi, koska yhden isäntäkoneen koko virtuaalista verkkoa voidaan valvoa yhden palomuurin avulla ja kaikkien uusien virtuaalikoneiden liikennettä voidaan valvoa automaattisesti ilman erillistä konfiguraatiota. Hypervisor-pohjaisten palomuurien

huonoja puolia ovat muun muassa teknologian uutuus ja sen tuomat uudet tietoturvahaasteet. Hypervisor on elintärkeä virtualisointialustan toiminnalle, ja tämä tekee siitä houkuttelevan hyökkäysvektorin. Onkin hyvin todennäköistä, että ennen pitkää tulee julki VMsafea ja muiden valmistajien hypervisor-rajapintoja vastaan suunnattuja hyökkäyksiä ja tietoturvauhkia. Hyödyt ovat silti haittoja selkeästi suuremmat, joten hypervisor-pohjaiset tietoturvaratkaisut tulevat todennäköisesti yleistymään, kun teknologia kypsyy.

5 Virtuaalinen testiympäristö

5.1 Topologia ja suunnitteluperiaatteet

Virtuaalisen StoneGate-palomuurin testausta varten rakennettiin pieni testiympäristö, joka koostui kahdesta tietokoneesta ja langattomasta reitittimestä. Isäntäkoneessa ajettiin VMware Workstation -ohjelmistoa, johon asennettiin virtuaaliset palomuurit ja yksi palvelin. Toiseen koneeseen asennettiin palomuurien hallintaohjelmisto StoneGate Management Center eli SMC. Koneet olivat yhteydessä internetiin langattoman reitittimen ja toisiinsa langattoman lähiverkon kautta. Testiympäristössä oli tarkoitus testata virtuaalisten palomuurien asennusta, hallintaa ja vikasietoisuutta. Tietoliikennettä tuotettiin testausta varten SMC-tietokoneen ja VM-CentOS-virtuaalikoneen avulla. VM-CentOS-koneen IP-osoite muunnettiin palomuuriklusterissa NAT:lla osoitteeksi 192.168.1.200, koska ilman NAT:ia näiden kahden koneen välisen liikenteen olisi pitänyt kulkea langattoman reitittimen kautta. Reitittimeen olisi pitänyt myös määrittää erikseen reitti vmnet3-verkkoon, koska se ei muuten olisi tietänyt, miten kyseiseen verkkoon pääsee. SMC asennettiin virtuaaliympäristön ulkopuolelle, koska näin pystyttiin testaamaan palomuurien siltausta isäntäkoneen verkkosovittimeen. Tällä tavalla pystyttiin myös testaamaan, että tietoliikenne todella toimii virtuaalisen ja fyysisen ympäristön välillä.



Kuvio 12. Testiympäristön looginen verkkotopologia.

Kuvio 12 esittää verkon topologian loogisella tasolla, fyysisellä tasolla kaikki langattomasta reitittimestä oikealla olevat komponentit ovat isäntäkoneen sisällä. Topologia vaatii kolme aliverkkoa, jotka on allokoitu yksityisestä IPv4-verkosta 192.168.0.0/16. Kaikille aliverkoille määriteltiin 24-bittinen verkkomaski selvyyden vuoksi. Tuotantoympäristössä maskit todennäköisesti määriteltäisiin tarvittavien IP-osoitteiden lukumäärän perusteella, ettei osoitteita tuhlattaisi. Virtuaalikytkimiä on käytössä kolme kappaletta. Vmnet0 on sillattu isäntäkoneen fyysiseen WLAN-verkkosovittimeen, eli sille ei voi määritellä omaa aliverkkoa. Vmnet0:aan yhdistetyille virtuaalisille verkkosovittimille määriteltiin IP-osoitteet siis fyysisen verkkosovittimen aliverkosta. Vmnet2:lle määriteltiin aliverkko 192.168.2.0/24, ja sen ainut tehtävä on yhdistää palomuurit toisiinsa klusteroinnin mahdollistamiseksi. Vmnet3 toimii virtuaalisena sisäverkkona, jolle määriteltiin aliverkko 192.168.3.0/24. Virtuaalikone VM-CentOS on yhdistetty vmnet3:een, jotta sen avulla voidaan testata yhteyksiä palomuuriklusterin läpi.

Palomuuriklusteria käytettiin normaalisti valmiustilassa, jossa yksi klusterin jäsen (engl. node) käsittelee liikennettä niin sanotussa yhteystilassa ja muut jäsenet ovat varalla valmiustilassa. Satunnaisesti valittu valmiustilassa oleva klusterin jäsen siirtyy yhteystilaan, jos havaitaan, että aikaisemmin yhteystilassa ollut jäsen ei enää välitä liikennettä. Valmiustila valittiin, koska kyseisen palomuuriohjelmiston version julkaisutietojen mukaan vain se on tuettu virtuaalisissa palomuureissa, tosin myös kuormanjakotilaa testattiin (25).

Klusteroinnin mahdollistamiseksi palomuurin normaalia liikennettä hoitavilla verkkosovittimilla on oltava kahdenlaisia IP-osoitteita: NDI eli Node Dedicated IP -osoite ja CVI eli Cluster Virtual IP -osoite. Yhdellä verkkosovittimella voi olla pelkkä NDI-osoite, pelkkä CVI-osoite tai useampi kappale molempia. NDI-osoitteet ovat palomuurikohtaisia, ja niitä käytetään, kun halutaan kommunikoida kyseisen palomuurin kanssa tai sen pitää avata itse yhteyksiä johonkin. Esimerkiksi palomuurille osoitetussa liikenteessä kohdeosoite on NDI-osoite ja palomuurin ottaessa itse yhteyttä jonnekin lähdeosoite on NDI-osoite. Virtuaalisten CVI-osoitteiden avulla usean palomuurin klusteri näyttää muiden verkkolaitteiden näkökulmasta yhdeltä loogiselta laitteelta. Yksi klusterin yhteystilassa olevista jäsenistä omistaa L2- ja L3-tason CVI-osoitteet eli CVI IP:n ja CVI MAC:n. Sekä CVI IP- ja MAC-osoitteet määritellään manuaalisesti. Virtuaaliset palomuurit tukevat virallisesti vain Packet Dispatch CVI -tilaa, jossa yksi klusterin jäsen eli liikenteenohjaaja (engl. dispatcher) omistaa CVI-osoitteet ja jakaa liikennettä tasaisesti kaikille klusterin jäsenille (25).

Kuormanjakotilassa olevassa klusterissa CVI MAC -osoitteeseen tarkoitetut paketit lähetetään liikenteenohjaajalle, joka määrittää laskemansa tiivistetaulun perusteella, mikä klusterin jäsen käsittelee kyseisen paketin. Päätöksen tehtyään, jos se ei käsittele pakettia itse, liikenteenohjaaja lähettää paketin jollekin klusterin jäsenelle saman verkkosovittimen kautta, josta se vastaanotti paketin. Yksi palomuuri käsittelee aina koko yhteyden alusta loppuun, eli olemassa oleviin yhteyksiin kuuluvat paketit siirretään aina saman palomuurin käsiteltäväksi. Valmiustilassa olevassa klusterissa yksi palomuuri luonnollisesti käsittelee kaikki paketit, koska se on yksin yhteystilassa. Liikenteenohjaajan mennessä yhteydettömään (engl. offline) tilaan toinen klusterin jäsen, eli uusi liikenteenohjaaja vaihtaa verkkosovittimensa MAC-osoitteen CVI MAC -osoitteeksi, jolloin CVI IP -osoitteeseen tuleva liikenne ohjautuu sille. Valmiustilassa olevassa klusterissa uusi liikenteenohjaaja siirtyy samalla myös yhteystilaan käsittelemään liikennettä. MAC-osoitteen vaihdon jälkeen uusi liikenteenohjaaja lähettää kyseisestä verkkosovittimesta niin sanotun gratuitous ARP -viestin. Viestin tarkoitus on saada kytkimet päivittämään MAC-taulunsa, jotta ne osaavat lähettää CVI MAC -osoitteeseen tarkoitetut kehykset oikealle palomuurille. (22.)

Taulukko 5. Palomuurien verkkosovittimien IP-osoitteet.

Verkkosovitin	Node 1 NDI	Node 2 NDI	Yhteinen CVI
eth0	192.168.1.11	192.168.1.12	192.168.1.13
eth1	192.168.2.1	192.168.2.2	-
eth2	192.168.3.1	192.168.3.2	192.168.3.3

Klusterin jäsenten verkkosovittimien IP-osoitteet on eritelty taulukossa 5. Jäsenten samannimisten verkkosovittimien NDI- ja CVI-osoitteiden on oltava samasta aliverkosta. Eth1-sovittimet määriteltiin yksinomaan heartbeat-verkoksi, joka ei tarvitse CVI-osoitetta, koska siinä ei ole muita verkkolaitteita kuin palomuurit. Suositellaan, että heartbeat-verkko omistetaan pelkästään heartbeat-liikenteelle. Yleensä se toteutetaankin fyysisissä palomuureissa ristikaapelilla, joka yhdistää klusterin jäsenten heartbeat-verkkosovittimet suoraan toisiinsa. Tässä tapauksessa heartbeat-verkolle on omistettu yksi virtuaalikytkin. Heartbeat-verkon kautta klusterin jäsenet vaihtavat ryhmälähetysliikenteenä tietoja tiloistaan ja käsittelemistään yhteyksistä. Heartbeat-liikenne eli tieto palomuurin omasta tilasta lähetetään oletuksena sekunnin välein ryhmälähetysosoitteeseen 225.1.1.1.

Jos jompikumpi jäsen kahden palomuurin klusterissa ei vastaanota heartbeat-liikennettä viiteen sekuntiin, se olettaa, että toinen jäsen on yhteydettömässä tilassa, jolloin se poistetaan klusterista väliaikaisesti. Tällöin kuormanjako-klusterissa aktiivinen jäsen ottaa itselleen CVI-osoitteet ja liikenteenohjaajan roolin. Valmiustilassa olevassa klusterissa se menee tämän lisäksi yhteystilaan. Tätä viiden sekunnin aikakatkaisuarvoa voi muuttaa mutta yleensä oletusarvoja ei tarvitse säätää, ellei heartbeat-verkko ole epäluotettava tai vaaditaan nopeampaa vikasietoisuutta. Heartbeat-verkon luotettavuus on hyvin tärkeää. Jos molemmat klusterin jäsenet luulevat, että toinen jäsen on hävinnyt klusterista, vaikka se käsitteleekin vielä liikennettä molemmat jäsenet käyttävät CVI-osoitteita ja yrittävät käsitellä kaiken liikenteen yksin. Tässä tilanteessa suurin osa liikenteestä ei todennäköisesti pääse klusterin läpi, koska palomuureissa kiinni olevat kytkimet näkevät saman MAC-osoitteen kahdessa eri portissa eivätkä osaa välittää paketteja oikein. (22.)

Heartbeat-verkossa lähetetään myös state sync -liikennettä eli tietoja kaikista klusterin jäsenten käsittelemistä yhteyksistä. Koko yhteystaulu lähetetään viiden sekunnin välein, ja inkrementaalisia päivityksiä lähetetään 50 millisekunnin välein ryhmälähetysosoitteeseen 225.1.1.2. State sync mahdollistaa saumattoman

vikasietoisuuden niin, että yhteydet eivät katkea, kun jokin klusterin jäsen vikaantuu. State syncin ansiosta kaikki klusterin jäsenet tietävät kaikki klusterin läpi kulkevat yhteydet, jolloin yhden jäsenen vikaantuessa toiset jäsenet pystyvät ottamaan sen aiemmin käsittelemät yhteydet hoitaakseen.

5.2 Vmware Workstationin asennus

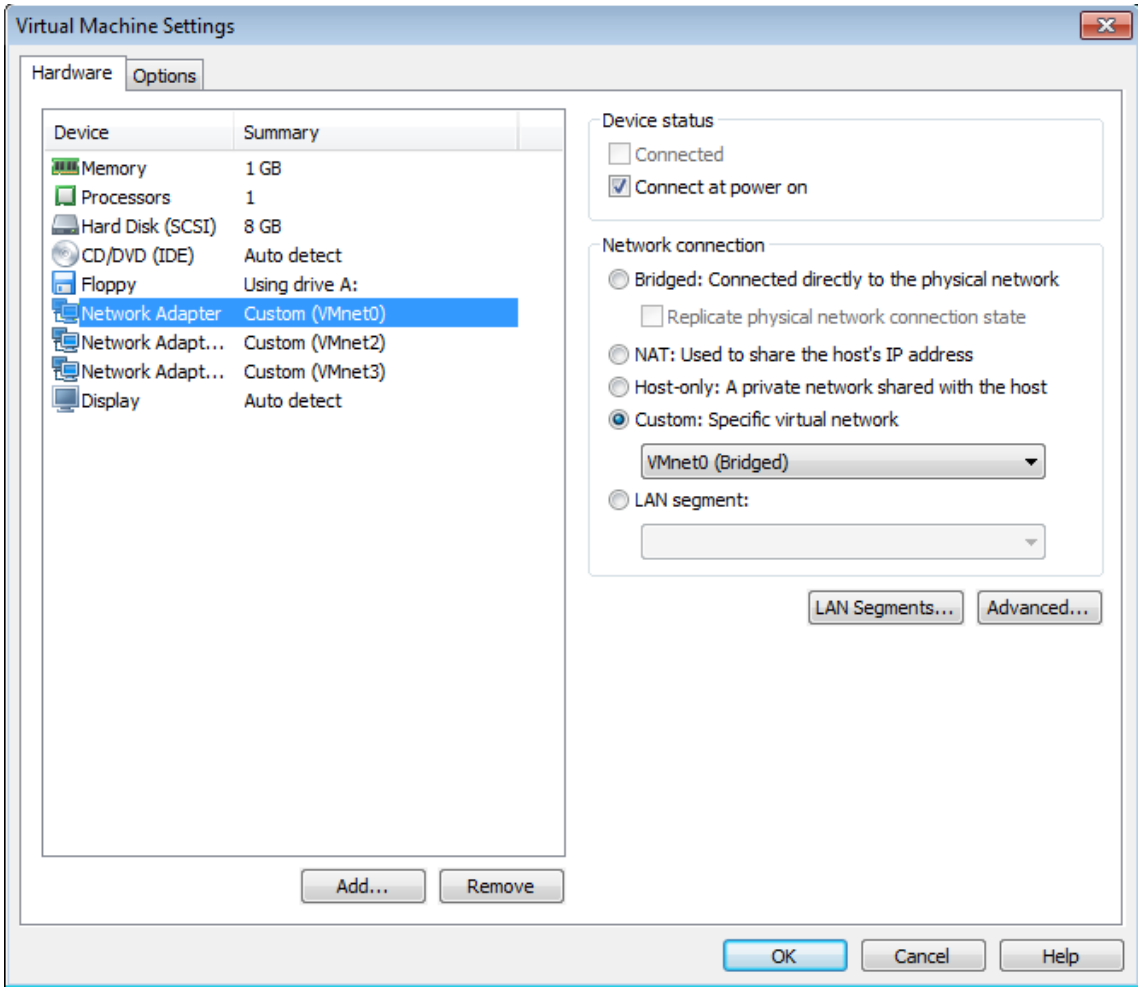
Testaukseen valittiin VMware Workstation 8.0, jonka asennus itsessään on hyvin suoraviivaista, joten sitä ei käydä sen tarkemmin läpi. Workstation 8:n asennus vaatii isäntäkoneelta 64-bittisen prosessorin ja kone täytti vaatimukset Intel Core i5 -prosessorilla ja 4 gigatavun RAM-muistilla. Hyvin lyhyet minimivaatimukset tarkoittavat sitä, että isäntäkoneen laitteisto on pääasiassa vain mitoitettava siinä ajettavien virtuaalikoneiden tarpeisiin. Prosessorin lisäksi RAM vaikuttaa eniten siihen, kuinka monta virtuaalikonetta voidaan ajaa samanaikaisesti. Neljä gigatavua riitti tähän testiympäristöön, koska VM-CentOS-koneelle allokoitiin 512 megatavua ja molemmille palomuureille 1024 megatavua RAM-muistia.

Virtuaalikoneita jaetaan yleisesti OVF eli Open Virtualization Format -formaatissa. OVF on suurimpien virtualisointiyhtiöiden vuonna 2007 alulle panema avoin standardi, jonka avulla virtuaalikoneen voi asentaa helposti samalla paketilla jopa usealle eri virtualisointialustalle (39). OVF-pakettiin kuuluu vähintään itse OVF-tiedosto ja yksi tai useampi virtuaalinen levy, jotka ovat VMwaren tuotteissa VMDK-tiedostoja. OVF-paketti voi siis sisältää myös useamman kuin yhden virtuaalikoneen. OVF-tiedosto on XML-muotoinen dokumentti, jossa virtuaalikoneen konfiguraatio on määritelty enemmän tai vähemmän tarkasti riippuen siitä, onko paketti tarkoitettu käytettäväksi yhdellä vai useammalla virtualisointialustalla tai alustan tietyllä versiolla. OVF:ssä määritellään muun muassa virtuaalikoneen käyttämä levytiedosto, verkkosovittimien konfiguraatio ja resurssien allokointi eli esimerkiksi muistin ja prosessorien määrä. OVF on siis vain virtuaalikoneiden levitystä ja siirtoa varten, virtuaalikoneita ei ajeta OVF-tiedostoista.

Tuomalla OVF-paketti esimerkiksi VMware Workstationiin ohjelmisto lukee virtuaalikoneen määritykset OVF-tiedostosta ja luo virtuaalikoneen käyttämällä sitä ja VMDK-tiedostoa. Luodun virtuaalikoneen konfiguraatio säilytetään isäntäkoneella tämän jälkeen VMX-tiedostossa ja levy uudessa VMDK-tiedostossa. Virtuaalikoneita

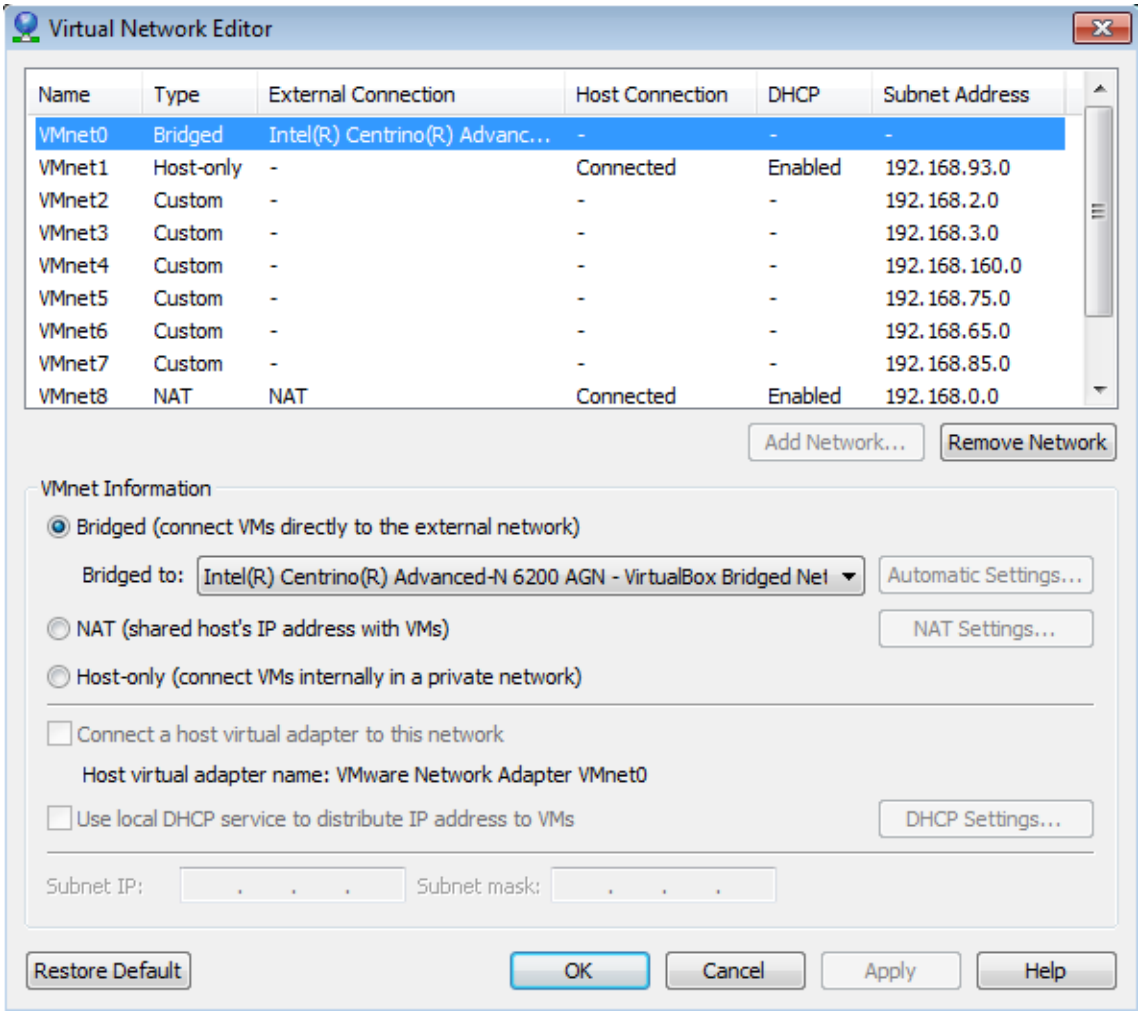
voidaan jakaa myös OVA eli Open Virtualization Format Archive -pakettina. OVA luodaan käytännössä pakkaamalla kaikki OVF-tiedostot yhteen tar-formaatissa olevaan pakettiin. OVA:n ainoa hyöty on siis se, että sen avulla virtuaalikoneita voidaan levittää helposti yhtenä tiedostona. StoneGate-virtuaalikonetta levitetään zip-tiedostona, joka sisältää OVF-, VMDK- ja MF-tiedostot. StoneGaten OVF määrittää virtuaalikoneelle muun muassa yhden gigatavun RAM-muistia, kahdeksan gigatavua kiintolevytilaa ja kolme verkkosovitinta vmxnet3-ajureilla. 120 megatavun kokoinen VMDK-levykuva sisältää palomuuriohjelmiston, ja MF-tiedosto sisältää tarkistussummat OVF- ja VMDK-tiedostoista niiden oikeellisuuden varmistamiseksi.

Valmista StoneGate-virtuaalikonetta oli yritetty testimielessä tuoda myös aiemmin asennettuun VMware Workstation 7:ään mutta yritys epäonnistui OVF:n yhteensopimattomuuden vuoksi. Virtuaalikone on luotu ESX Server 4:llä, joka käyttää OVF 1.0-versiota ja Workstation 7 ei ymmärrä OVF 0.9-versiota uudempia tiedostoja. OVF olisi pitänyt muuntaa Workstation 7:n kanssa yhteensopivaksi VMware Converter -työkalulla mutta siinä vaiheessa jo aiemmin suunniteltu päivitys Workstation 8 -versioon oli järkevämpää. Asennettu StoneGate-palomuurin versio 5.3.2 vaatii vähintään VMware ESX 3.5.0 tai ESXi 4.1 -alustan. Asennettaessa palomuureja VMware Workstation 8:aan kävi selväksi, että ne ovat senkin kanssa yhteensopivia, koska Workstation 8 käyttää muun muassa samoja OVF- ja VMX-versioita kuin esimerkiksi ESXi 4.1.



Kuvio 13. StoneGate-palomuurin virtuaalikoneen asetukset.

Virtuaalikoneiden tuonti VMware Workstationiin oli parin minuutin prosessi, jossa OVF-tiedosto piti vain avata ja antaa ohjelmiston luoda siitä uusi virtuaalikone. Näin asennettiin kaksi virtuaalikonetta, koska tarkoitus oli käyttää kahta palomuuria samanaikaisesti. Virtuaalikoneiden asetukset jätettiin oletusarvoihinsa mutta verkkosovittimet asetettiin haluttuihin virtuaalikytkimiin, kuten kuviossa 13 näkyy. Virtuaalikoneiden oletusnimien perään liitettiin ”node 1” ja ”node 2”, jotta palomuurit pystyisi erottamaan helposti toisistaan. VM-CentOS-virtuaalikone luotiin yksinkertaisesti tekemällä uusi virtuaalikone ja valitsemalla asennusmediaksi aiemmin ladattu CentOS 5.7 -ISO-tiedosto.



Kuvio 14. Virtuaalikytkimien verkkoasetukset VMware Workstationissa.

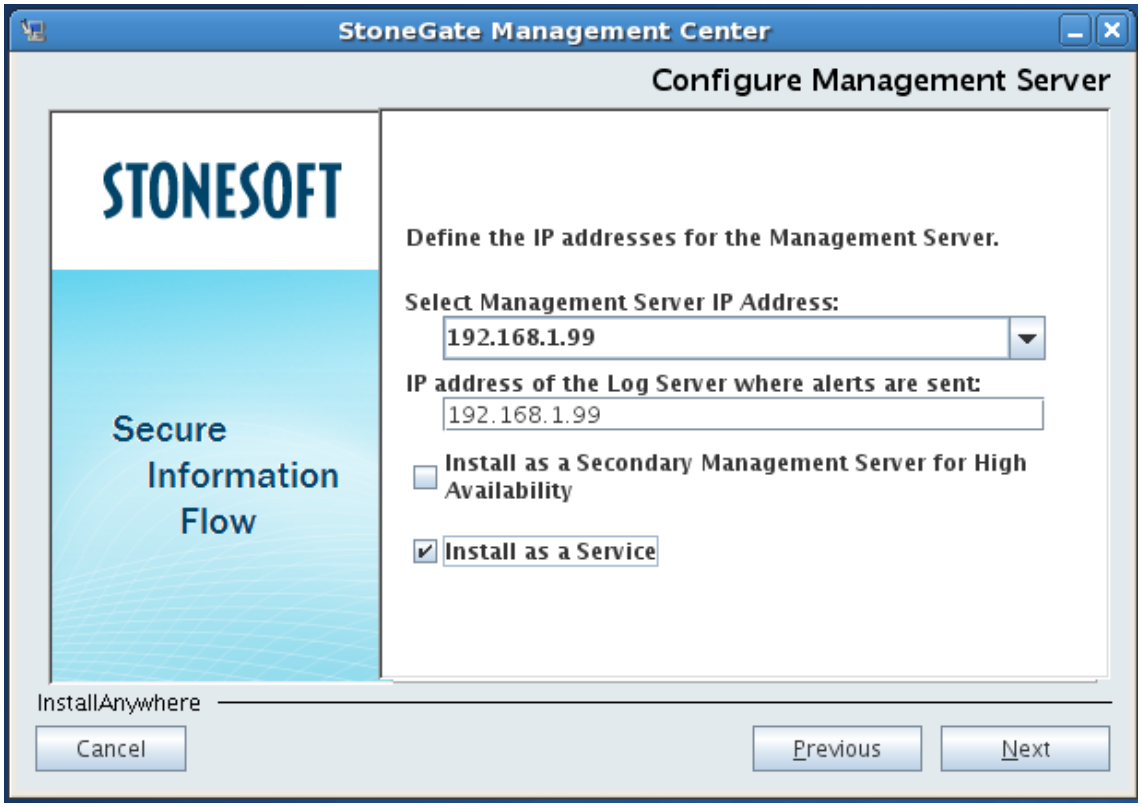
Aiemmin tehtyjen asetusten lisäksi oli enää tarpeen määrittää oikeat aliverkot virtuaalikytkimille, joka onnistui klikkaamalla Workstationissa Edit-valikkoa ja avaamalla sen alta ”Virtual Network Editor”-työkalu. Aliverkot määriteltiin kytkimille vmnet2 ja vmnet3 kuvion 14 mukaisesti. Aliverkkojen määritys on tosin tarkkaan ottaen tarpeen vain käytettäessä virtuaalikytkimien DHCP-palvelimia. Vmnet0 määriteltiin sillatuksi kytkimeksi ja sillattu fyysinen verkkosovitin määriteltiin käsin. Oletusarvoisesti Workstation päättää siltaukseen käytettävän fyysisen verkkosovittimen automaattisesti mutta testattaessa VM-CentOS-virtuaalikoneen verkkoyhteyksiä automatiikka valitsi väärän sovittimen. Verkkoyhteydet eivät tämän takia tietenkään toimineet, joten vmnet0 määriteltiin eksplisiittisesti siltaamaan isäntäkoneen langattomaan verkkosovittimeen, joka oli mallia Intel Centrino Advanced-N 6200 AGN. Isäntäkoneelle on myös asennettu ilmainen virtualisointiohjelmisto VirtualBox, joka on sitonut omat virtuaaliset verkkosovittimensa koneen fyysisiin sovittimiin. Tämän takia fyysisen

sovittimen nimen perässä lukee myös VirtualBoxin vmnet0:aa vastaavan sovittimen nimi.

5.3 StoneGate Management Centerin asennus

SMC asennettiin 32-bittiselle kannettavalle tietokoneelle, joka täytti laitteiston osalta ohjelmiston vaatimukset (37). Tietokoneessa oli Intel Core2 Duo -prosessori ja kolme gigatavua RAM-muistia. Käyttöjärjestelmänä oli Ubuntu 10.04 LTS, vaikka se ei ole SMC:n virallisesti tuettujen käyttöjärjestelmien listalla. Syynä oli se, että CentOS 5 ei suostunut asentumaan koneelle jonkin yhteensopimattomuuden vuoksi. SMC tuntui silti toimivan Ubuntussa ilman ongelmia.

SMC-asennus käsittää vähintään Management ja Log Server -palvelimet, jotka voidaan asentaa samalle koneelle, kuten tässä tapauksessa tehtiin. Log Server vaatii periaatteessa 50 gigatavua muistia mutta sitä pystyttiin varaamaan SMC:lle vain 20 gigatavua rajallisen kiintolevytilan takia. Tämän lisäksi swap-osiolle omistettiin kolme gigatavua. Tämänkaltaisessa testiympäristössä vähäisen muistin ei pitäisi haitata, koska lokidataa tulee hyvin vähän ja itse SMC-asennus vaatii vain 650 megatavua tilaa. Toinen vaihtoehto SMC:tä asentaessa on palvelimien eriyttäminen, joka on hyvä idea suuremmissa ympäristöissä jos logidataa tulee hyvin paljon. SMC:tä käytetään Management Clientillä, jolla kirjaudutaan Management Server -palvelimelle sisään ja hallitaan järjestelmää graafisen käyttöliittymän kautta. Valittiin tyypillinen asennus, jossa Management Client asennettiin SMC-koneelle suosituksen mukaisesti (38). Pelkän Management Clientin voi myös asentaa erikseen muihinkin tietokoneisiin samalla asennuspaketilla.



Kuvio 15. Kuvankaappaus yhdestä SMC:n asennusvaiheesta.

SMC:n asennus aloitettiin lataamalla SMC 5.3.2 Linux-asennuspaketti eli zip-tiedosto, joka purettiin tietokoneelle. Asennus käynnistetään ajamalla asennuskansiosta löytyvä setup.sh-skripti. Oli tarpeen asentaa vain välttämättömimmät komponentit eli Management ja Log Server -palvelimet ja Management Client, joten valittiin tyypillinen asennus. Tämän jälkeen myös kuviossa 15 esitetyt tärkeimmät syötteet olivat palvelimien IP-osoitteet ja valinta, että asennetaanko palvelimet palveluina. Palvelimet asennettiin palveluina, koska näin ne käynnistyvät automaattisesti tietokoneen käynnistyessä. Log Serverin TCP-porttia voi myös vaihtaa tässä vaiheessa mutta se jätettiin oletusarvoonsa, joka on 3020. Asennuksen yhteydessä on myös pakko luoda yksi käyttäjätunnus, jolla SMC:hen kirjaudutaan ensimmäisen kerran sisään. Luodulla käyttäjällä on SMC:hen laajimmat superuser-tason oikeudet. Käyttäjiä voi luoda asennuksen jälkeen lisää ja niille voi määritellä eri tasoisia oikeuksia.

Kuvio 16. Kuvankaappaus Management Clientin kirjautumisikkunasta.

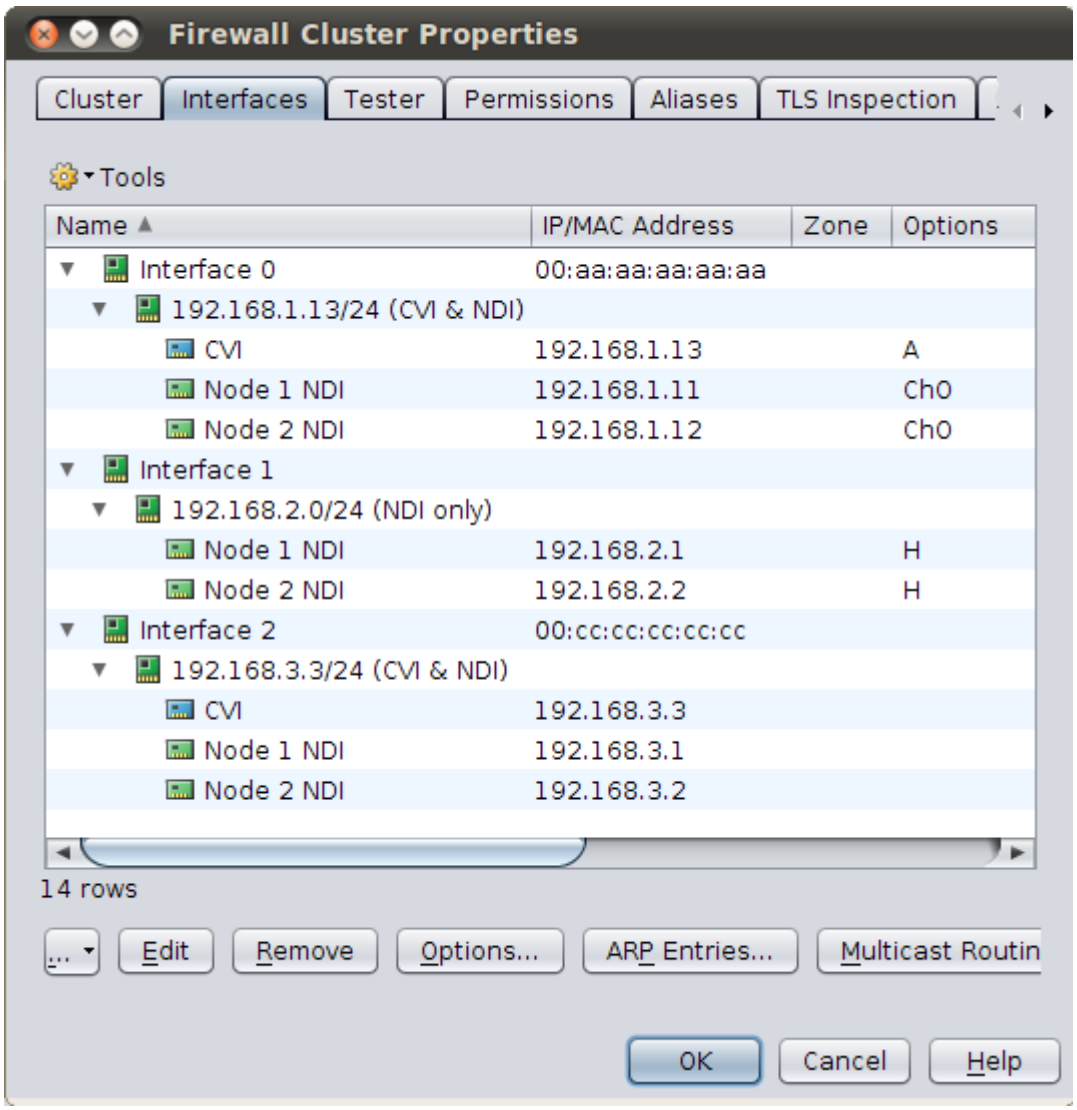
Asennuksen jälkeen järjestelmään kirjaudutaan sisään kuvion 16 mukaisesti Management Clientilla aiemmin luodulla käyttäjätunnuksella. Clientin saa auki suorittamalla sgClient.sh-skriptin, joka löytyy muiden oleellisten skriptien lailla asennuskansion bin-alikansiosta. Oletusasennuskansio, jota myös käytettiin tässä tapauksessa, on Linuxissa /usr/local/stonegate. Käyttäjätunnus tosin ehti jo unohtua tässä vaiheessa, joten sgCreateAdmin.sh-skriptillä luotiin uusi tunnus. Tällaisten skriptien takia pääsyä SMC-koneelle ja sen root-salasanaan on hyvä rajoittaa tiukasti.

Sisäänkirjautumisen jälkeen ensimmäinen välttämätön toimenpide on SMC-lisenssin asentaminen, koska ilman sitä järjestelmässä ei pysty tekemään juuri mitään. Tätä varten generoitiin testilisenssi, joka sidottiin SMC:n IP-osoitteeseen. Lisenssille lasketaan automaattisesti generoinnin yhteydessä tunnistusta varten yksilöllinen Proof of License eli POL-koodi. Ainut ongelma asennuksen yhteydessä liittyi lisenssiin, kun SMC ei suostunut hyväksymään sitä. SMC-kone oli yhteydessä verkkoon WLAN-sovittimen kautta, joka oli määritelty toimimaan DHCP-tilassa. DHCP-palvelin oli konfiguroitu antamaan kyseiselle WLAN-sovittimelle MAC-osoitteen perusteella aina sama IP-osoite 192.168.1.99. IP ei näin ollen ikinä muuttunut, vaikka se tuli DHCP:ltä. Verkkoasetuksia tarkistettaessa IP näytti aina olevan oikea, joten kesti hetken huomata, että se olikin asetettu DHCP:llä. Lisenssi suostui asentumaan, kun sama IP-osoite asetettiin staattisesti.

5.4 Palomuurien käyttöönotto SMC:n kanssa

Palomuurien saattamiseksi toimintakuntoon on tehtävä tämän jälkeen vielä kolme toimenpidettä. Ensin palomuurielementit on luotava SMC:ssä, toiseksi palomuureista on otettava yhteys SMC:hen ja kolmanneksi niihin on asennettava tietoturvapolitiikka eli säännöstö (37). SMC:n graafinen käyttöliittymä on melko intuitiivinen, joten elementtien luonti onnistui nopeasti. Palomuurien konfiguraationäkymään päästään napsauttamalla Configuration-valikosta Firewall-nimikettä. Klusterielementti luotiin napsauttamalla näkymää hiiren oikealla painikkeella ja valitsemalla New-valikosta Firewall Cluster -nimike. Klusterille annettiin nimeksi StoneGate Virtual Cluster ja sille määriteltiin verkkosovittimet Interfaces-välilehdeltä.

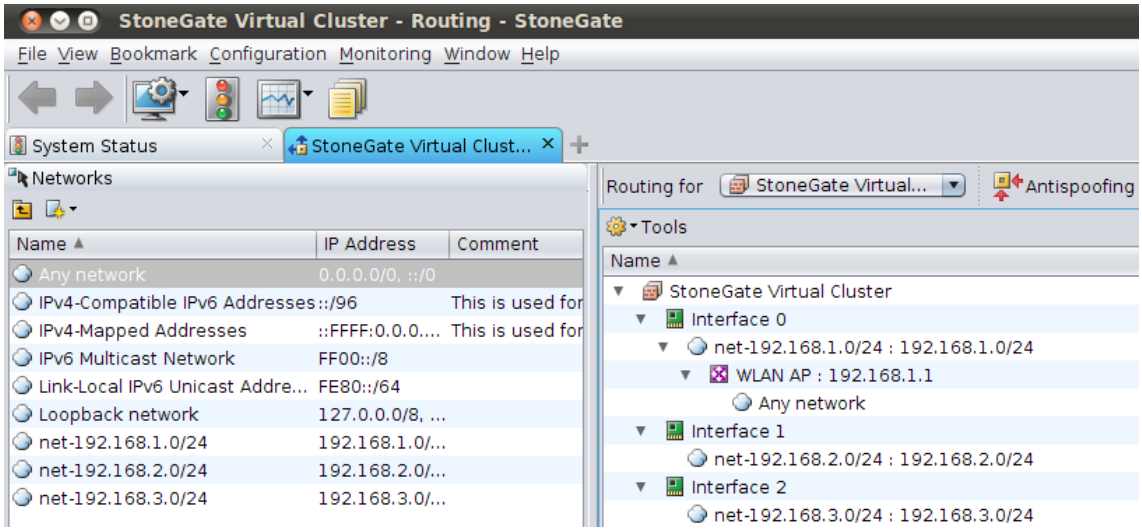
Valmiiksi määritetyt sovittimet näkyvät kuviossa 17, NDI- ja CVI-osoitteet määritettiin suunnitellun topologian mukaisesti. Heartbeat-verkot määriteltiin Options-valikossa, jossa eth1 valittiin ensisijaiseksi ja eth0 toissijaiseksi heartbeat-verkoksi. Heartbeat-verkot näkyvät kuviossa 17 myös Options-sarakkeen alla, jossa iso H-kirjain tarkoittaa ensisijaista ja pieni h-kirjain toissijaista verkkoa. Kontrollisovitin tarkoittaa verkkosovitinta, jota SMC käyttää kommunikoidessaan palomuurien kanssa. Kontrollisovitin oli pakko määrittää sillatuksi eth0-sovittimeksi, koska se oli testiympäristössä ainut reitti, jota kautta palomuurit pystyivät saamaan yhteyden SMC-koneeseen. Ensisijainen kontrollisovitin identifioidaan Options-sarakkeessa isolla C-kirjaimella, toissijaista sovitinta ei määritetty, koska eth0 on ainut mahdollinen reitti SMC-koneeseen. Klusteri määritettiin vielä Advanced-välilehdellä toimimaan valmiustilassa oletusarvoisen kuormanjakotilan sijasta.



Kuvio 17. Klusterin verkkosovittimien konfigurointi.

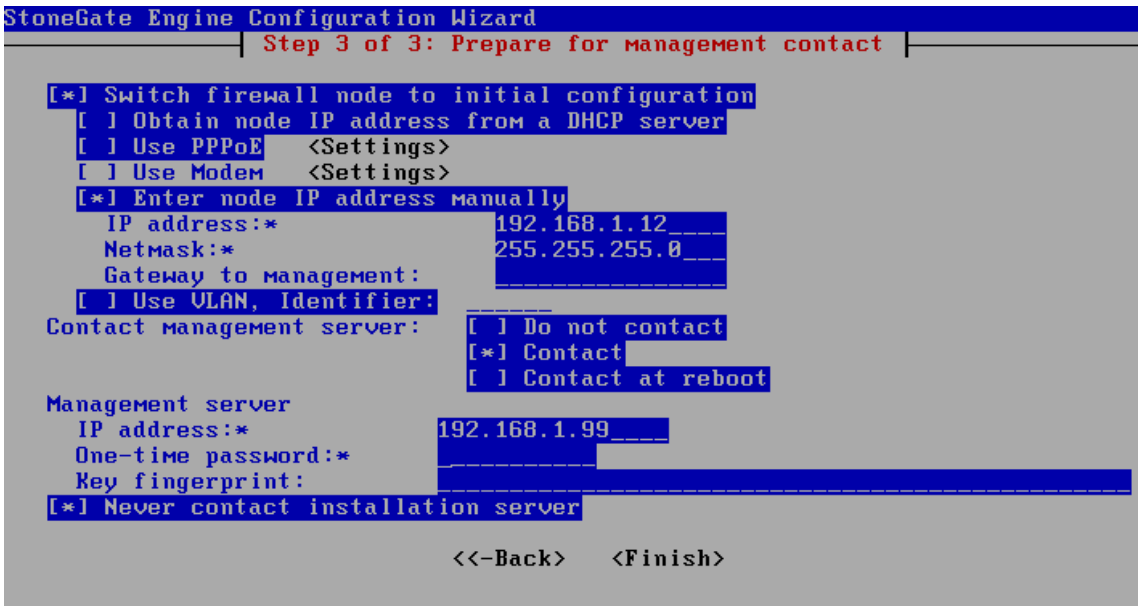
Klusterielementti oli periaatteessa käyttövalmis verkkosovittimien määrittelyn jälkeen, jos ei oteta lukuun reititysasetuksia. SMC avaa elementin tallennuksen jälkeen ponnahdusikkunan reitityksen konfiguroinnista, jota napsauttamalla pääsee suoraan kyseisen elementin reititysnäkymään. Näin yksinkertaisessa topologiassa oli tarpeen määrittää klusterille vain oletusreitti. Tätä varten luotiin reititinelementti, joka kuvastaa oletusyhdyskäytävää. Yhdyskäytävä oli tässä tapauksessa WLAN AP -reititin, joten elementille annettiin nimeksi WLAN AP ja IP-osoitteeksi 192.168.1.1. Reititinelementti vedettiin hiirellä eth0:n verkon alle ja sen alle vedettiin valikosta ”Any network”-verkkoelementti, joka vastaa verkkoa 0.0.0.0/0. Reititysnäkymä on melko helppolukuinen kuten kuviosta 18 näkyy. Reititinelementin tai verkkosovittimen alle laitetaan sen takana olevat verkot, ja reititinelementtiä käytettäessä se osoittaa, minkä

laitteen kautta kyseisiin verkkoihin pääsee. SMC taas luo tästä konfiguraatiosta tekstimuotoisen reititystaulun, kun säännöstö asennetaan palomuureihin.



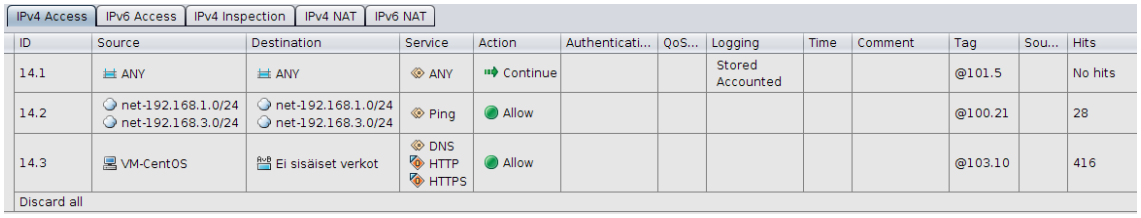
Kuvio 18. Klusterin reitityskonfiguraatio SMC:ssä.

Palomuurit on seuraavaksi yhdistettävä SMC:hen eli suoritettava ”initial contact” SMC:n kanssa. Tätä varten SMC:ssä on ensin luotava palomuureille kertakäyttöiset salasanat valitsemalla klusterin Configuration-kontekstivalikosta Save Initial Configuration. Palomuurien virtuaalikoneet laitettiin käyntiin ensimmäistä kertaa, jolloin ne käynnistyvät suoraan konfigurointivalikkoon. Kuviossa 19 esitetyssä kolmannessa valikkoruudussa asetettiin palomuuri ”initial configuration”-tilaan ja syötettiin tärkeimmät asetukset eli IP-osoitteet ja kertakäyttöinen salasana. Tästä eteenpäin varsinaisen säännöstön asennukseen asti palomuurilla on käytössä hyvin yksinkertainen säännöstö, joka sallii vain hallintayhteydet itsensä ja SMC:n välillä. Konfigurointivalikosta poistumisen jälkeen palomuuri luo itselleen yksityisen RSA-avaimen ja ottaa yhteyttä SMC:hen, jolta se saa varmenteen. Kyseistä varmennetta käytetään tästä eteenpäin todentamaan kaikki palomuurin ja SMC:n välinen kommunikaatio. Tahot luottavat toistensa varmenteisiin, koska ne ovat kaikki saman SMC-koneella sijaitsevan varmentajan eli Certificate Authorityn allekirjoittamia.



Kuvio 19. Node 2:n alustava konfiguraatio.

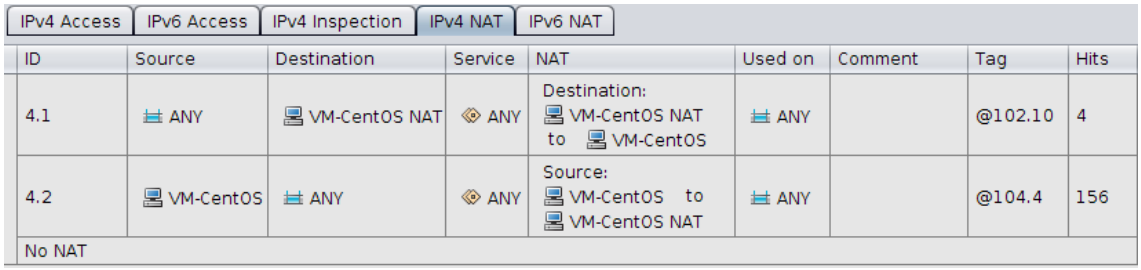
Tietoturvapolitiikka tehtiin sellaiseksi, että se salli testaukseen tarvittavat yhteydet mutta torjui muut. Kuvio 20 havainnollistaa SMC:n intuitiivista sääntökäyttöliittymää, joka on jaoteltu IPv4- ja IPv6-pääsylistoihin ja NAT- ja tutkintasääntöihin. Kuviossa 20 ensimmäisenä näkyvä IPv4 Access -sääntö on continue-sääntö, jolla aktivoidaan lokitus kaikille sitä seuraaville säännöille. Continue-sääntöjen asetukset voi myös halutessaan ylikirjoittaa sitä seuraavissa yksittäisissä säännöissä. Seuraava sääntö sallii ping-paketit testiympäristön verkkojen välillä lukuun ottamatta heartbeat-verkko, jotta voitiin testata päästä päähän -yhteyksiä laitteiden välillä. Viimeinen sääntö sallii HTTP-, HTTPS- ja DNS-liikenteen VM-CentOS-koneen ja internetin välillä. ”Ei sisäiset verkot”-ekspressio esittää internetiä ja koostuu loogisesta lausekkeesta ”NOT 192.168.1.0/24 OR 192.168.2.0/24 OR 192.168.3.0/24” eli se on testiympäristön verkkojen negaatio.



Kuvio 20. Säännöstön IPv4 Access -sääntöjen välilehti.

Kuviossa 21 näkyvä ensimmäinen NAT-sääntö muuntaa VM-CentOS-koneen NAT-osoitteeseen tulevien pakettien kohdeosoitteet koneen oikeaksi osoitteeksi eli

osoitteesta 192.168.1.200 osoitteeksi 192.168.3.10. Toinen NAT-sääntö muuntaa VM-CentOS-koneesta lähetettyjen pakettien lähdeosoitteet koneen NAT-osoitteeksi eli osoitteesta 192.168.3.10 osoitteeksi 192.168.1.200. Jokaisen säännöstön on pakko pohjautua johonkin mallipohjaan, joten lueteltujen sääntöjen lisäksi säännöstö sisältää myös oletusmallipohjan säännöt. Oletusmallipohja sallii muun muassa kaikki tarpeelliset yhteydet palomuurin ja SMC:n välillä. Kuvioiden 20 ja 21 Hits-sarakkeessa näkyy sääntöihin osuneiden pakettien lukumäärä, koska kuvakaappaukset säännöistä otettiin politiikan asennuksen ja testauksen jälkeen.



Kuvio 21. Säännöstön IPv4 NAT -sääntöjen välilehti.

Säännöstön asennuksen yhteydessä SMC ensin validoi sen eli tarkistaa, löytyykö siitä selkeitä konfigurointivirheitä. Tällaisia ovat esimerkiksi puuttuvat määritykset, kuten lähde- tai kohdeosoite, ja väärät määritykset, kuten säännössä viitattu VPN, jota ei ole konfiguroitu kyseiselle palomuurille tai kaksi identtistä sääntöä. Tämän jälkeen SMC rakentaa palomuurikohtaiset konfiguraatiot, kuten säännöstön ja reititystaulun. Varsinkin moni oletusmallipohjan sääntö käyttää alias-elementtejä, joilla viitataan esimerkiksi kyseisen muurin kaikkiin NDI-osoitteisiin. SMC selvittää aliakset säännöstön asennuksen yhteydessä ja kirjoittaa niiden IP-osoitteet eksplisiittisesti palomuurille lähetettäviin konfiguraatiotiedostoihin.

Validoinnin ja konfiguraation rakentamisen jälkeen itse valmis säännöstö ladataan palomuureille, ja ne ottavat sen käyttöön. Tämän jälkeen SMC odottaa, että palomuurit ottavat siihen yhteyttä, kun niillä on uusi säännöstö käytössä. Yhteyden epäonnistuessa palomuurit palaavat takaisin vanhaan säännöstöön, jolla yhteys onnistui. Varotoimi on olemassa, jottei konfiguraatiovirhe estä palomuurin hallitsemista. Yhteyden onnistuessa säännöstön asennus on valmis, ja se on käytössä palomuureissa. Palomuurien ottaessa käyttöön hyvin laajaa säännöstöä ne eivät käsittele liikennettä muutamaan sekuntiin mutta normaalin säännöstön asennuksen

aikana häiriö on minimaalinen. Pieni katkos voi tulla myös muutettaessa verkkosovittimien konfiguraatiota, koska palomuurin on silloin alustettava sovittimet uudestaan. Pakettihäviötä testattiin lähettämällä ping-viestejä säännöstön asennuksen aikana palomuurin läpi VM-CentOS-koneesta SMC-koneelle. Säännöstön asennus sääntöjen muuttamisen jälkeen ei tuottanut pakettihäviötä. Säännöstön asennus heartbeat-verkon verkkosovittimen IP-osoitteen muutoksen jälkeen tuotti yhden paketin häviön. Tämä ei vielä vaikuta yhteyksiin merkittävästi, koska TCP-yhteydet selviävät yleensä hyvin jopa 10—20 sekunnin katkoksista.

Yhteyksiä ja asennettua säännöstöä testattiin ping-, wget- ja tcpdump-komennoilla. Ensin varmistettiin, että ping-paketit menivät perille vain haluttujen verkkojen eli 192.168.1.0/24 ja 192.168.3.0/24 välillä. Testin tulokset näkyvät esimerkkitestissä 1.

```
[root@vm-centos ~]# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
--- 192.168.2.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms

[root@vm-centos ~]# ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.
64 bytes from 192.168.3.1: icmp_seq=1 ttl=64 time=1.10 ms
64 bytes from 192.168.3.1: icmp_seq=2 ttl=64 time=0.231 ms

[root@vm-centos ~]# ping 192.168.1.99
PING 192.168.1.99 (192.168.1.99) 56(84) bytes of data.
64 bytes from 192.168.1.99: icmp_seq=1 ttl=63 time=12.9 ms
64 bytes from 192.168.1.99: icmp_seq=2 ttl=63 time=2.52 ms
```

Esimerkkitesti 1. Access-sääntöjen testaus ping-komennolla.

Wget-komennot ajettiin VM-CentOS-koneessa ja niiden avulla saatiin selville, että HTTP-, HTTPS- ja DNS-yhteydet toimivat internetiin. Komennon tulosteesta nähtiin, että verkkosivujen IP-osoitteet pystyttiin selvittämään DNS:n avulla ja HTTP- ja HTTPS-yhteydet toimivat, koska sivut pystyttiin lataamaan. Testin tulokset näkyvät esimerkkitestissä 2.

```
[root@vm-centos ~]# wget http://www.metropolia.fi
--2012-02-10 06:57:19--  http://www.metropolia.fi/
Resolving www.metropolia.fi... 195.148.144.10
Connecting to www.metropolia.fi|195.148.144.10|:80... connected.
HTTP request sent, awaiting response... 200 OK

[root@vm-centos ~]# wget https://mail.metropolia.fi
--2012-02-10 07:11:06--  https://mail.metropolia.fi/
Resolving mail.metropolia.fi... 195.148.166.17
Connecting to mail.metropolia.fi|195.148.166.17|:443...
connected.
HTTP request sent, awaiting response... 302 Found
```

Esimerkkitesti 2. Access-sääntöjen testaus wget-komennolla.

Tcpdump-komennolla tallennettiin liikennettä SMC- ja VM-CentOS-koneilla samanaikaisesti, kun koneesta toiseen lähetettiin ping-viestejä. NAT-sääntöjen toimivuus pystyttiin varmistamaan katsomalla tallenteista, miten VM-CentOS-koneen IP-osoite muuttui matkalla.

```
[root@vm-centos ~]# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96
bytes
07:03:33.933422 IP 192.168.3.10 > 192.168.1.99: ICMP echo
request, id 30999, seq 1, length 64
07:03:33.943349 IP 192.168.1.99 > 192.168.3.10: ICMP echo reply,
id 30999, seq 1, length 64
```

```
lauri@smc:~$ sudo tcpdump -i wlan0 -n icmp
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on wlan0, link-type EN10MB (Ethernet), capture size 96
bytes
17:03:34.737953 IP 192.168.1.200 > 192.168.1.99: ICMP echo
request, id 30999, seq 1, length 64
17:03:34.742165 IP 192.168.1.99 > 192.168.1.200: ICMP echo
reply, id 30999, seq 1, length 64
```

Esimerkkitesti 3. NAT-sääntöjen testaus tcpdump-komennolla.

Testin tulokset näkyvät esimerkkitestissä 3. VM-CentOS-koneen tallenteesta näkyy, että paketin lähdeosoite oli alun alkaen 192.168.3.10. SMC-koneen tallenteesta taas näkyy, että lähdeosoite on muuttunut klusterin läpi mentyään NAT-osoitteeksi 192.168.1.200. Aikaero tallenteissa selittyy sillä, että koneiden kellot olivat eri aikavyöhykkeillä eikä niitä ollut synkronoitu.

5.5 Klusterin vikasietoisuuden testaus

Klusterin vikasietoisuutta testattiin sekä hallitusti, että hallitsemattomasti ensin valmius- ja sitten kuormanjakotilassa. Hallitussa tilanteessa aktiivinen palomuuri käskettiin SMC:ssä yhteydettömään tai valmiustilaan tai käynnistymään uudelleen. Hallitsemattomassa tilanteessa aktiivisen palomuurin virtuaalikone suljettiin suoraan VMware Workstationissa. Molemmissa tilanteissa tarkasteltiin, miten toimenpide vaikutti liikenteeseen klusterin läpi, koska teoriassa yhteyksien siirtymisen toiselle palomuurille ei pitäisi näkyä peruskäyttäjille millään tavalla. Toisessa osiossa klusteri muutettiin ensin toimimaan kuormanjakotilassa, jonka jälkeen suoritettiin samat testit uudestaan. Testaukseen käytettiin jatkuvasti lähetettäviä ping-viestejä VM-CentOS-koneesta SMC:hen, viestejä lähetettiin sekunnin välein. Edellä mainittujen testien tulokset on esitelty taulukossa 6.

Taulukko 6. Korkein havaittu pakettihäviö eri vikasietoisuustesteissä

Skenaario	Valmiustila	Kuormanjakotila
Käsky yhteydettömään tai valmiustilaan	2	0
Käsketty uudelleenkäynnistys	2	0
Virtuaalikoneen sulkeminen	4	4

Valmiustilassa tehdyissä testeissä havaittiin, että hallittu menetelmä onnistui hyvin. Usean testin perusteella aktiivisen palomuurin käskeminen yhteydettömään tai valmiustilaan aiheutti korkeintaan yhden tai kahden paketin häviön. Aktiivisen palomuurin uudelleenkäynnistys SMC:n kautta ei aiheuttanut yhtään enempää häviötä. Virtuaalikoneen yhtäkkinen sammuminen aiheutti jo neljän paketin häviön. Virtuaalikone voisi sammua esimerkiksi siinä tilanteessa, jos klusterin jäsenet olisivat eri isäntäkoneissa ja toinen näistä koneista sammuisi esimerkiksi sähkökatkon takia. Klusteri saatiin kerran hieman epämääräiseen tilaan, kun toinen palomuuri meni aikakatkaisutilaan, eli SMC ei saanut siihen yhteyttä. Molempia palomuureja oli käsketty useamman kerran lyhyen ajan sisällä eri tiloihin ennen tätä. Tilanne lopulta korjaantui itsestään mutta osoitti, että SMC ei pysty estämään kaikkia huonoja konfiguraatioyhdistelmiä.

SMC estää standby-komennon lähetyksen aktiiviselle palomuurille, kun klusterin toinen jäsen on yhteydettömässä tilassa, koska viimeistä aktiivista palomuuria ei voi laittaa valmiustilaan. SMC toisaalta taas sallii molempien palomuurien käskemisen peräjälkeen yhteydettömään tilaan, jolloin kumpikaan ei siis käsittele liikennettä. Palomuuri voi siirtyä yhteydettömään tilaan myös automaattisesti, jos esimerkiksi jokin konfiguroitu testi epäonnistuu. Yhteydettömässä tilassa oleva elementti on käskettävä takaisin esimerkiksi valmiustilaan manuaalisesti. Kyseinen tila onkin pääasiassa tarkoitettu esimerkiksi huoltokatkoksiin, jolloin palomuurin ohjelmistoa päivitetään. Vikasietoisuus toimi hyvin klusterin ollessa valmiustilassa ja palomuurit määrittelivät tilansa automaattisesti klusterin toisen jäsenen tilan mukaan aivan oikein. Kun aktiivinen palomuuri A käynnistettiin uudelleen, palomuuri B meni yhteystilaan ja käynnistyttyään uudelleen palomuuri A meni automaattisesti valmiustilaan.

Creation time	Sender	Src Addr	Dst Addr	Service	IP Prot...	Src Port	Dst Port	State
2012-02-11 16:04:10	StoneGate Virtual Cluster node 2	192.168.3.10	192.168.1.99	Echo Request (No Code)	ICMP			ICMP echo
2012-02-11 16:01:16	StoneGate Virtual Cluster node 1	192.168.1.99	192.168.1.11	SG Commands	TCP	55171	4987	TCP established
2012-02-11 16:01:38	StoneGate Virtual Cluster node 2	192.168.1.99	192.168.1.12	SG Commands	TCP	39599	4987	TCP established
2012-02-11 15:33:11	StoneGate Virtual Cluster node 1	192.168.1.11	192.168.1.99	SG Log	TCP	33226	3020	TCP established
2012-02-11 15:21:55	StoneGate Virtual Cluster node 1	192.168.1.11	192.168.1.99	SG Log	TCP	59770	3020	TCP established
2012-02-11 16:02:18	StoneGate Virtual Cluster node 2	192.168.1.12	192.168.1.99	SG Log	TCP	42122	3020	TCP established
2012-02-11 15:24:51	StoneGate Virtual Cluster node 2	192.168.1.12	192.168.1.99	SG Log	TCP	50753	3020	TCP established
2012-02-11 16:00:56	StoneGate Virtual Cluster node 2	192.168.1.11	225.1.1.2	SG State Sync (Multicast)	UDP	38172	3001	UDP established
2012-02-11 16:00:56	StoneGate Virtual Cluster node 2	192.168.1.11	225.1.1.2	SG State Sync (Multicast)	UDP	47895	3000	UDP established
2012-02-11 16:00:56	StoneGate Virtual Cluster node 2	192.168.1.12	225.1.1.2	SG State Sync (Multicast)	UDP	59141	3000	UDP established

Kuvio 22. Listaus klusterin testaushetkellä käsittelemistä yhteyksistä.

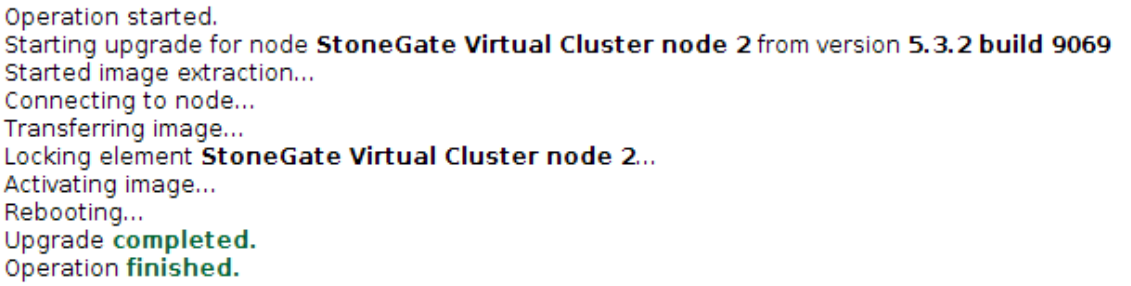
Klusteri muutettiin seuraavaksi toimimaan kuormanjakotilassa ja säännöstö asennettiin uudestaan, jotta muutos tulisi voimaan. VM-CentOS-koneella aloitettiin taas jatkuva ping-komento ja katsottiin SMC:n kuviossa 22 näkyvästä klusterin yhteyslistasta, mikä palomuuri käsittelee yhteyttä. Tässä tapauksessa yhteyttä käsitteli node 2, joka käskettiin seuraavaksi yhteydettömään tilaan. Toimenpide ei aiheuttanut yhtään pakettihäviötä. Sama prosessi toistettiin, paitsi tällä kertaa yhteyttä käsittelevä palomuuri käynnistettiin SMC:n kautta uudestaan. Hallittu uudelleenkäynnistyskään ei aiheuttanut pakettihäviötä, kuten oli odotettavissa. Viimein suljettiin yhteyttä käsittelevä virtuaalikone VMware Workstationissa, jonka seurauksena nähtiin neljän paketin häviö.

Testien tuloksena valmius- ja kuormanjakotilojen vikasietoisuudessa ei nähty merkittävää eroa. Kuormanjakotilassa yhteydet siirtyivät palomuurilta toiselle hieman nopeammin mutta se oli odotettavissa, koska toinen palomuuri oli silloin jo valmiiksi aktiivinen. Valmiustilassa toisen palomuurin on ensin aktivoiduttava, joka tuo prosessiin hieman lisää viivettä. VM-CentOS-koneella tehtyjen testien perusteella palomuurit ja virtualisointialusta eivät myöskään vaikuttaneet negatiivisesti latenssiin tai latausnopeuksiin. Tämä vahvistettiin ajamalla sama internetistä löytyvä nopeustesti VM-CentOS-, SMC- ja isäntäkoneella useamman kerran. Kaikkien kolmen koneen testien tulokset olivat hyvin lähellä toisiaan. Tehdyn testauksen perusteella klusterin toiminnan ja vikasietoisuuden voitiin sanoa toimivan kaiken kaikkiaan erittäin hyvin. Kyseiset testit olivat silti hyvin rajoitettuja testiympäristön koon takia, joten saavutettujen tulosten perusteella voidaan vahvistaa vain tuotteen toimivuus testatun kaltaisessa ympäristössä. Tuotantoympäristöön verrattavissa olevia tuloksia saataisiin testaamalla useammalla päätelaiteparilla, suuremmilla liikennemäärillä ja samoilla protokollilla kuin tuotannossa käytetään. Nyt jätettiin testaamatta esimerkiksi usein käytetyt VPN- ja Multi-Link-ominaisuudet. Tämän opinnäytetyön tarkoituksiin saavutetut tulokset olivat kuitenkin riittävät.

5.6 Käyttötapaus klusterin päivitys

Palomuuriohjelmiston päivitys toimii samalla tavalla virtuaalisissa ja fyysisissä StoneGate-palomuureissa. Yksi klusteroinnin eduista on se, että oikein tehtynä huoltokatkot, kuten ohjelmiston päivitykset, eivät häiritse liikennettä millään tavalla. Taustalla on luonnollisesti oletus, että jos klusteria käytetään kuormanjakotilassa, niin aktiiviseksi jäävät palomuurit pystyvät käsittelemään ylimääräisen liikenteen. Päivitysprosessi on itsessään hyvin yksinkertainen ylläpitäjälle. Uusi ohjelmisto ladataan ensin joko SMC:n kautta tai Stonesoftin verkkosivuilta. Jos oletusasetuksia ei muuteta, SMC tarkistaa uudet päivitykset Stonesoftin palvelimilta tunnin välein. SMC todentaa itsensä palvelimille omalla POL-koodillaan ja palvelin tarkastaa, että kyseisen koodin tukisopimus on voimassa ennen yhteyden hyväksymistä. Kun päivitys on ladattu SMC:hen päivitettävä palomuuri on käskettävä yhteydettömään tilaan. Itse päivitys voidaan tehdä yhdellä kertaa tai osissa, eli päivityksen voi halutessaan ladata palomuurille etukäteen ja aktivoida sen myöhempänä ajankohtana. Toinen vaihtoehto on päivityksen lataus ja aktivointi yhdellä kertaa, jolloin palomuuri käynnistetään uudelleen heti latauksen jälkeen. Päivitysprosessi aloitettiin tuomalla versio 5.3.3:n asennuspaketti SMC:hen ja käynnistämällä päivitys palomuurin kontekstivalikosta. Päivitys ja aktivointi valittiin seuraavasta valikosta suoritettavaksi yhdellä kertaa. (40.)

Itse päivityspaketti on sama kaikilla alustoilla, koska tieto muun muassa palomuurin alustasta on kirjoitettu palomuurissa lukutilassa olevalle root-levyosiolle. Kyseinen tieto on olennainen, koska sen pitää vastata lisenssissä määritettyä alustaa. Itse ohjelmisto eli palomuurin käyttöjärjestelmä tallennetaan erilliselle levyosiolle. Palomuuri säilyttää kiintolevyllään nykyisen ja edellisen version käyttöjärjestelmästä, mikä mahdollistaa esimerkiksi vikatilanteissa aiemman version nopean palautuksen. Palautus onnistuu uudelleenkäynnistämällä palomuuri edellisen version levyosiolta joko valitsemalla se GRUB-valikossa tai syöttämällä komento sg-toggle-active komentorivillä. Kuvio 23 on SMC:n esitys päivitystehtävästä, joka kesti pari minuuttia. Sen aikana päivitys asennettiin ja palomuuri uudelleenkäynnistettiin uuteen versioon.



Kuvio 23. SMC:n tuloste palomuurin onnistuneesta päivityksestä.

Säännöstö suositellaan asentamaan palomuureihin uudestaan päivitysten jälkeen, koska se voi muuttua hieman versioiden välillä. Esimerkiksi tietty asetus tai sen syntaksi on voitu toteuttaa uuden version säännöstössä hieman eri tavalla jonkin ohjelmistovirheen korjaamiseksi. Tämä on erityisen totta varsinkin SMC:n päivityksen jälkeen. Säännöstö asennettiin klusteriin ja testattiin, että kaikki sallitut yhteydet toimivat edelleenkin kuten ennenkin. Palomuurien komentoriveillä ajettu komento sg-version vahvisti myös, että käytössä oli uusi versio 5.3.3.

6 Yhteenveto

Opinnäytetyössä selvitettiin ensin tietoverkkojen ja palomuurien historiaa ja teoriapohjaa, jonka jälkeen keskityttiin virtualisointiin ja virtuaalisen testiympäristön toteutukseen. Palomuurit ovat kehittyneet parissa kymmenessä vuodessa yksinkertaisista pakettisuodattimista älykkäiksi ja monipuolisiksi sovelluspalomuureiksi, jotka tarjoavat useita teknologioita tietoliikenteen turvaamiseen ja seulontaan. Stonesoft Oyj:n valmistama tilallinen sovelluspalomuuri StoneGate Firewall/VPN on yksi näistä niin sanotuista seuraavan sukupolven palomuureista. Virtualisointi on myös kehittynyt ja yleistynyt nopeasti viime vuosina, mikä on tuonut uusia tietoturvahaasteita. Virtualisointi jaoteltiin työssä kahteen eri tyyppiin, eli hosted- ja hypervisor-arkkitehtuureihin pohjautuviin virtualisointialustoihin. Hypervisor-virtualisointialustoja, kuten VMware ESXi:tä, käytetään paljon palvelimien virtualisointiin. Monet palvelimia virtualisoineet yritykset ovat havahtuneet myöhään siihen tosiasiaan, että virtualisointi ei vähennä palvelimien tietoturvan tarvetta millään tavalla. Virtuaaliympäristöjen tietoturvaa on paljolti ylenkatsottu mutta sen tarpeeseen ollaan pikku hiljaa heräämässä. Monet tietoturvavalmistajat ovat hypänneet tähän

kelkkaan mukaan tarjoten erilaisia virtuaalisia tietoturvaratkaisuja virustorjunnasta palomuureihin. Yksi näistä valmistajista on Stonesoft, jonka virtuaalista StoneGate-palomuuria testattiin tämän työn aikana.

Virtuaaliset tietoverkot toimivat hieman eri tavalla kuin perinteiset fyysiset verkot, minkä takia virtualisointialustojen valmistajat ovat julkistaneet tai ovat julkistamassa tehokkaampia tekniikoita virtuaalisten verkkojen hallintaan. Yksi näistä tekniikoista on VMwaren julkistama VMsafe, joka tarjoaa rajapintoja muun muassa virtuaaliympäristön verkkoliikenteen kokonaisvaltaiseen tarkasteluun suoraan hypervisorissa. StoneGate on tässä mielessä perinteinen palomuuri, että sen on pakko olla liikennevirran keskellä pystyäkseen valvomaan sitä. Se ei siis pysty käyttämään hypervisor-rajapintoja hyödykseen. VMsafea käyttäviä tietoturvaratkaisuja on julkistettu vasta hyvin vähän mutta sen kaltaiset tekniikat tulevat olemaan tärkeässä asemassa virtuaalisen tietoturvan kehityksessä tulevaisuudessa.

Virtuaalinen testiympäristö suunniteltiin niin, että sillä voitiin testata palomuurien perustoiminnallisuutta. Toteutuksessa asennettiin VMware Workstationiin virtuaaliset palomuurit ja toiseen tietokoneeseen StoneGate Management Center palomuurien hallintaa varten. Testiympäristön toteutuksen yhteydessä selvitettiin myös tarkemmin, miten StoneGate-palomuurien klusterointi ja niiden hallinta toimii. Virtuaalisten palomuurien suorituskyky ja hallittavuus todettiin hyväksi. Parhaita puolia olivat helppo käyttöönotto ja hallittavuus sekä saumaton integroituminen olemassaolevaan fyysiseen StoneGate-infrastruktuuriin. Huonoiksi puoliksi todettiin rajattu skaalautuvuus VMsafe-tuen puutteen vuoksi. Sen takia StoneGate-palomuurien sijainti virtuaalisessa verkossa on päätettävä tarkasti, jonka takia verkon hallinta monimutkaistuu. Toinen huono puoli oli se, että Stonesoft tarjoaa vain 32-bittistä virtuaalipalomuuria, kun taas korkeampaa suorituskykyä haluaville 64-bittinen virtuaalikone on hyvin tärkeä ominaisuus. Kaiken kaikkiaan testit osoittivat, että tuote toimii tällaisessa ympäristössä hyvin, joskin oikeat tuotantotestit vaatisivat paljon laajempaa ja pidempiaikaista testausta.

Lähteet

1 Odom, Wendell. 2008. CCENT/CCNA ICND1 Official Exam Certification Guide. Indianapolis: Cisco Press.

2 The default MTU sizes for different network topologies. Verkkodokumentti. Microsoft Corporation. <http://support.microsoft.com/kb/314496> Luettu 23.10.2011.

3 TCP/IP Networks – The Internet Model. Verkkodokumentti. <http://www.citap.com/documents/tcp-ip/tcpip012.htm> Luettu 27.10.2011.

4 TCP/IP-protokollat. Verkkodokumentti. Matti Rintala. <http://koti.mbnet.fi/mrin/paattotyo/tcp_ip.html> Luettu 29.10.2011.

5 CIDR Notation – Classless Inter Domain Routing. Verkkodokumentti. About.com. <http://compnetworking.about.com/od/workingwithipaddresses/a/cidr_notation.htm> Luettu 29.10.2011.

6 Odom, Wendell. 2008. CCNA ICND2 Official Exam Certification Guide. Indianapolis: Cisco Press.

7 The IPv6 Header and How it Works. Verkkodokumentti. IPv6.com Inc. <http://ipv6.com/articles/general/IPv6-Header.htm> Luettu 29.10.2011.

8 IPv6 Tunneling and other Transition Mechanics. Verkkodokumentti. IPv6.com Inc. <http://ipv6.com/articles/gateways/IPv6-Tunnelling.htm> Luettu 30.10.2011.

9 Firewall and Internet Security – The Internet Protocol Journal – Volume 2, No. 2. Verkkodokumentti. Fred Avolio. <http://www.cisco.com/web/about/ac123/ac147/ac174/ac200/about_cisco_ipj_archive_article09186a00800c85ae.html> Luettu 1.11.2011.

10 CERT-FI. Verkkodokumentti. CERT-FI. <http://www.cert.fi> Luettu 1.11.2011.

11 Firewall. Verkkodokumentti. Tech-FAQ. <http://www.tech-faq.com/firewall.html> Luettu 3.11.2011.

12 Evolution of the Firewall Industry. Verkkodokumentti. Cisco Systems. <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm> Luettu 4.11.2011.

13 Greene, Tim. The evolution of application layer firewalls. Verkkodokumentti. Network World. <http://www.networkworld.com/news/2004/0202specialfocus.html> Luettu 4.11.2011.

14 Firewall Policy. Verkkodokumentti. Northwestern University. <http://www.it.northwestern.edu/policies/firewall.html> 24.6.2010. Luettu 5.11.2011.

15 Architecture with Multiple Layers of Firewalls. Verkkodokumentti. Home Automation - JAEC. <http://www.jaec.info/Automation-Computer-Security/computer-gadgets/computer-security/firewalls-vpn/architecture-layers-firewalls> 4.2.2009. Luettu 5.11.2011.

16 What is QoS?: Quality of Service (QoS). Verkkodokumentti. Microsoft Corporation. <http://technet.microsoft.com/en-us/library/cc757120%28WS.10%29.aspx> 28.3.2003. Luettu 8.11.2011.

17 Stonesoft Vuosikertomus 2010. Verkkodokumentti. Stonesoft Oyj. <http://www.stonesoft.com/export/download/financial_files/Stonesoft_Vuosikertomus_2010_FI.pdf> Luettu 9.11.2011.

18 About Us - Stonesoft. Verkkodokumentti. Stonesoft Oyj. <http://www.stonesoft.com/en/about_us> Luettu 9.11.2011.

19 Stonesoft Oyj | Pörssitiedote. Verkkodokumentti. Stonesoft Oyj. <http://www.kauppalehti.fi/5/i/porssi/tiedotteet/porssitiedote.jsp?id=201110030094&comid=SFT> 3.10.2011. Luettu 9.11.2011.

20 Check Point Software:Stonesoft's StoneBeat FullCluster. Verkkodokumentti. Check Point Software Technologies Ltd. <http://www.checkpoint.com/press/partners/2000/stonesoft101000.html> 10.10.2000. Luettu 14.11.2011.

21 StoneGate Provides Firewall/VPN Security for the Mainframe. Verkkodokumentti. PR Newswire Association LLC. <http://www2.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/01-22-2003/0001876476&EDATE=> 22.1.2003. Luettu 14.11.2011.

22 StoneGate 5.3 Firewall Reference Guide. Verkkodokumentti. Stonesoft Oyj. <http://www.stonesoft.com/export/download/sg_man/StoneGate_Firewall_Reference_Guide_v5-3.pdf> 16.9.2011. Luettu 14.11.2011.

23 StoneGate NextGen Firewall Appliance Comparison Datasheet. Verkkodokumentti. Stonesoft Oyj. <http://www.stonesoft.com/export/download/pdf/datasheet_stonegateFW-allInOne.pdf> Luettu 14.11.2011.

24 StoneGate Virtual Security Solutions. Verkkodokumentti. Stonesoft Oyj. <http://www.stonesoft.com/export/download/pdf/StoneGate_virtual_security_solutions_web_letter.pdf> Luettu 26.11.2011.

25 StoneGate Firewall/VPN Release Notes for Version 5.3.2. Verkkodokumentti. Stonesoft Oyj. <https://my.stonesoft.com/support/attachment.do?docid=6963&file=FW_5.3.2-RLNT.pdf> 24.10.2011. Luettu 26.11.2011.

26 Hammersley, Eric. 2007. Professional VMware Server. Indianapolis: Wiley Publishing Inc.

27 Data Centers: How to cut carbon emissions and costs. Verkkodokumentti. McKinsey & Company. <http://www.mckinsey.com/clientservice/bto/pointofview/pdf/BT_Data_Center.pd> 2008. Luettu 2.12.2011.

28 Oglesby, Ron; Herold, Scott; Laverick, Mike. 2008. VMware Infrastructure 3: Advanced Technical Design Guide and Advanced Operations Guide. The Brian Madden Company.

29 Workstation User's Manual VMware Workstation 7.0. Verkkodokumentti. VMware Inc. <http://www.vmware.com/pdf/ws7_manual.pdf> Luettu 16.12.2011.

30 Puustinen, Johanna. 2010. Fyysinen palvelin hakkaa virtuaalisen tietoturvassa. Verkkodokumentti. Tietoviikko. <http://www.tietoviikko.fi/kaikki_uutiset/article384906.ece> 11.4.2010. Luettu 28.12.2011.

31 New VMware VMsafe™ Technology Allows the Virtual Datacenter to Be More Secure Than Physical Environments. Verkkodokumentti. VMware Inc. <http://www.vmware.com/company/news/releases/vmsafe_vmworld.html> 27.2.2008. Luettu 6.1.2012.

32 What actually is VMsafe and the VMsafe API?. Verkkodokumentti. VMware Inc. <http://blogs.vmware.com/vcloud/2010/04/what-actually-is-vmsafe-and-the-vmsafe-api.html> 20.4.2010. Luettu 6.1.2012.

33 MacDonald, Neil. 2009. Don't let VMware Become Internet Explorer. Verkkodokumentti. <http://blogs.gartner.com/neil_macdonald/2009/06/29/dont-let-vmware-become-internet-explorer/> 29.6.2009. Luettu 13.1.2012.

34 vGW Series Virtual Gateway - Virtualization Firewall Security for Data Centers and Cloud Networks. Verkkodokumentti. Juniper Networks Inc. <http://www.juniper.net/us/en/products-services/software/security/vgw-series/> Luettu 14.1.2012.

35 Virtualization Security Technology – Data Center Virtualization – Deep Security. Verkkodokumentti. Trend Micro Inc. <http://us.trendmicro.com/us/products/enterprise/datacenter-security/deep-security/index.html> Luettu 14.1.2012.

36 Luoma, Juha. 2012. Firewall/VPN Product Manager, Stonesoft Oyj, Helsinki. Sähköposti 16.1.2012.

37 StoneGate Management Center Release Notes for Version 5.3.2. Verkkodokumentti. Stonesoft Oyj. <https://my.stonesoft.com/support/attachment.do?docid=6865&file=SMC_5.3.2-RLNT.pdf> 21.9.2011. Luettu 28.1.2012.

38 StoneGate Management Center Installation Guide v5.3. Verkkodokumentti. Stonesoft Oyj. <http://www.stonesoft.com/export/download/sg_man/StoneGate_Management_Center_Installation_Guide_v5-3.pdf> 27.6.2011. Luettu 28.1.2012.

39 DMTF Accepts New Format for Portable Virtual Machines from Virtualization Leaders. Verkkodokumentti. DMTF Inc. <http://dmtf.org/news/pr/2007/9/dmtf-accepts-new-format-portable-virtual-machines-virtualization-leaders> 10.9.2007. Luettu 4.2.2012.

40 StoneGate 5.3 Firewall/VPN Installation Guide. Verkkodokumentti. Stonesoft Oyj. <http://www.stonesoft.com/export/download/sg_man/StoneGate_Firewall_Installation_Guide_v5-3.pdf> 7.9.2011. Luettu 11.2.2012.